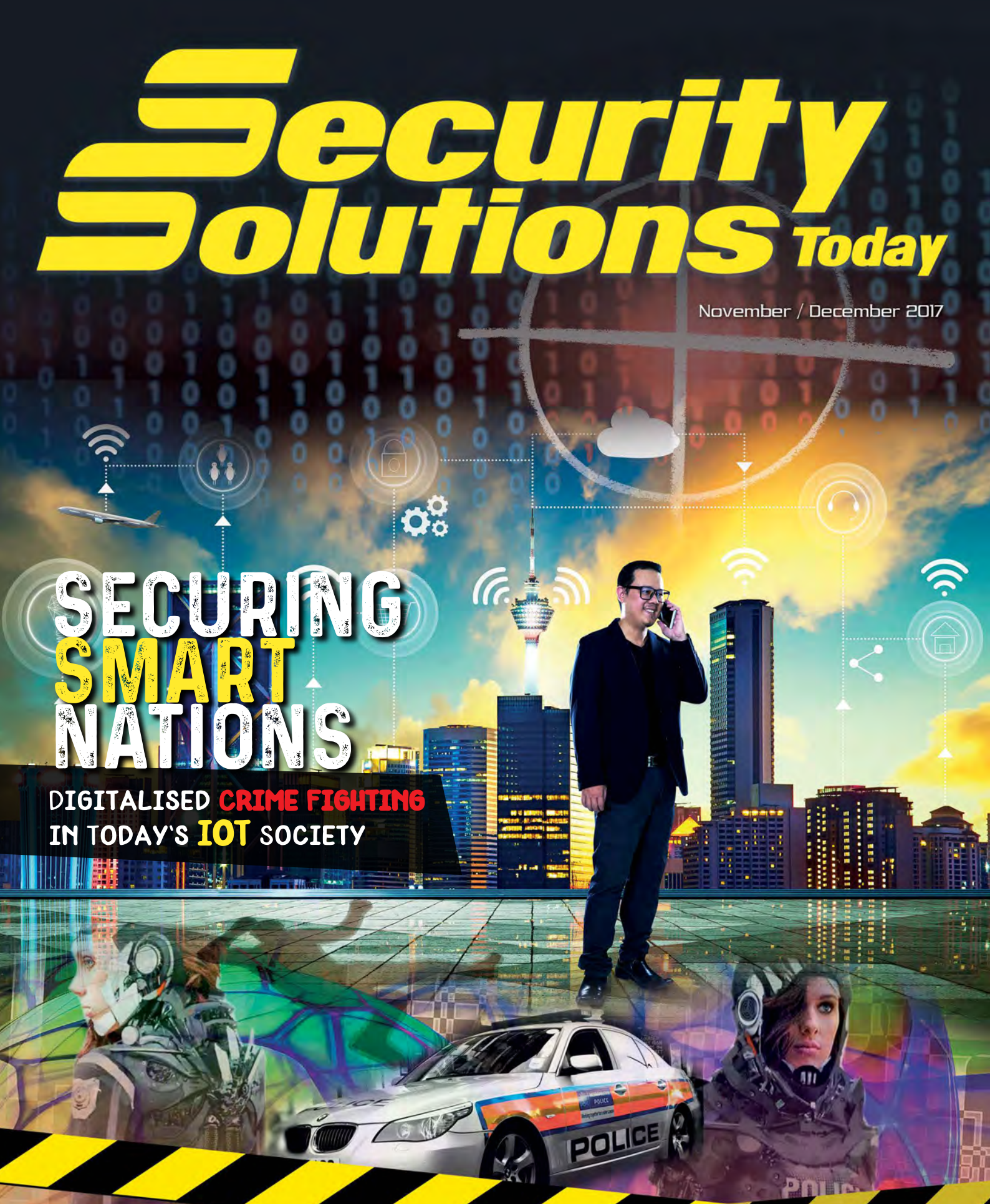
Security Solutions Today

November / December 2017



SECURING SMART NATIONS

DIGITALISED CRIME FIGHTING IN TODAY'S IOT SOCIETY

Cover Focus

Smart Cities–Safe Cities: Intelligent Cities

Security Features

Lip Reading CCTV Coming Soon to Supermarkets!

Product Feature

Dahua's Drones Surveil SMART Cities

Scan this code to visit our website

All-in-one Design Replaces Multiple Conventional Cameras

Multi-sensor panoramic camera greatly reduces deployment costs

- Replace multiple single-sensor cameras and save on installation & maintenance costs
- Multiple image sensors and 1 IP address, superior low light performance
- Seamless splicing technology for flawless image
- 180° / 360° viewing angle without image distortion
- Smart Tracking automatically follows subjects of interest
- All models rated IP67 & IK10, designed for outdoor applications

H.265 | 180°/360° Panoramic | TRACKING Smart Tracking | Starlight | WDR | IP67 | Vandal-proof

Comprehensive line up for every job:

IPC-PFW8800-A180
4x2MP Multi-Sensor Panoramic Network IR Bullet Camera

IPC-PDBW8800-A180
4x2MP Multi-Sensor Panoramic Network IR Dome Camera

PSD8802-A180
4x2MP Multi-Sensor Panoramic Network Camera+PTZ Camera

PSD81602-A360
8x2MP Multi-Sensor Panoramic Network Camera+PTZ Camera

CE FC UL RoHS ISO 9001:2000

DAHUA TECHNOLOGY SINGAPORE PTE. LTD.
Add: 62 Ubi Road 1 #06-15 Oxley Biz Hub 2
Singapore 408734
E-mail: sales.sg@global.dahuatech.com

HD300 High Security
Electronically-Controlled Barrier

DSC720
High Security Bollard

DSC1200 High Strength
Surface Mounted Barricade

DSC2000
High Security Barricade

DSC501
High Security Barricade

DSC288 High Security
Sliding Gate

DSC207 High Security
Shallow Foundation Barricade

DSC7000 High Security
Beam Barrier

DSC600 High Security Shallow
Foundation Fixed Bollard

DSC1100 High Strength
Portable Barrier

TT207SFM High Security
Surface-Mounted Barricade

DSC7500 High Security
Swing Beam Barrier

TT212 High Strength
Beam Barricade

TT280 High Security
Linear Crash Gate

Delta
Keeps Them Stopped!

18,000+ Systems Deployed Around the World!

Stopping a bomb-laden car and SUV from penetrating the entrance to a consulate to guarding against vehicle assaults at dams, border crossings, court houses, embassies, capitol buildings, palaces, hotels, headquarters buildings and many other types of important facilities, Delta's bollards, barricades, beams, barriers, gates and guard booths keep vehicles stopped, keeping people and property safe in over 130 countries throughout the world since 1974.

DELTA

Go to **www.deltascientific.com** for full details & specifications.

40355 Delta Lane, Palmdale, CA 93551 ▲ **1-661-575-1100** ▲ **info@deltascientific.com**

IN THIS ISSUE

6 **CALENDAR OF EVENTS**

8 **EDITOR'S NOTE**

10 **IN THE NEWS**
Updates from Asia & Beyond

36 **FUN FACTS**
Crime Fighting Goes Digital

42 **APPLICATION STORIES**
Bodycams, Biometric Identiity & more

54 **FUN FACTS**
Policing SMART Cities Around the World

56 **CASE STUDIES**
IoT Surveillance, SMART Policing & Other Public Safety Solutions

75 **ALL ABOUT IOT & CYBER SECURITY**
Security goes Digital with Cyber Solutions & SMART Robots

76 **FUN FACTS**
Robo - cops Around the World

100 **SECURITY FEATURES**
Stepping up on Security with CCTV Drones, Lip Recognition CCTV & More

133 **INSIDE LOOK**
Lockdown on Data Security with Encryption & Cloud Protection

139 **IN FOCUS**
Spotlight on industry Experts from BAE Systems & Carbon Black

150 **PRODUCT SHOWCASE**
Tech Toys Gallore with Wi-Fi® Indoor Video Camera, SMART 7-in-1 Door Station & more

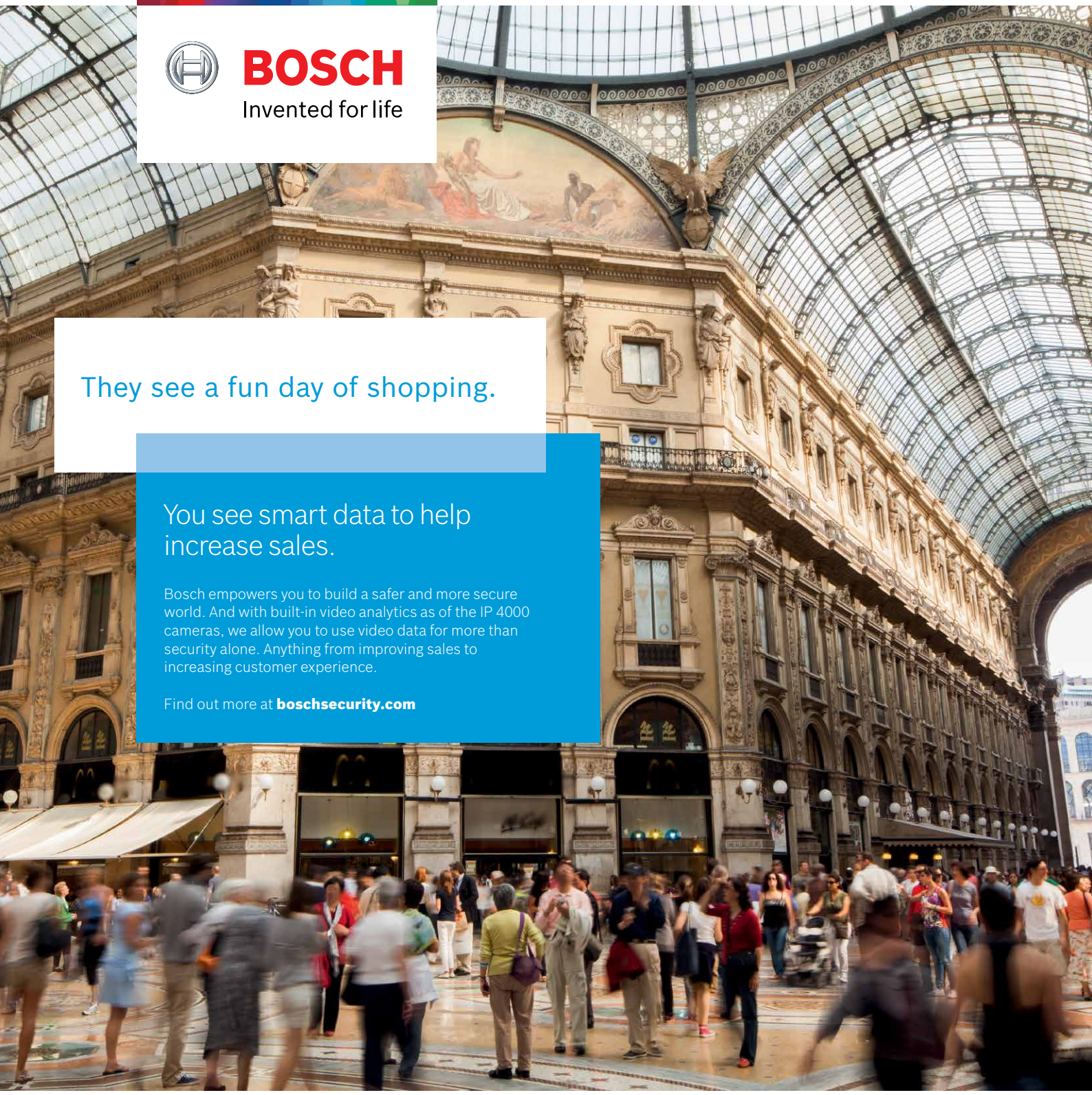
154 **EDITOR'S AFTERTHOUGHT**
Fighting Crime in SMART Nations of the Future

38 **COVER FOCUS**
Smart Cities–Safe Cities: Intelligent Cities

145 **SPECIAL PRODUCT FEATURE**
Dahua on the Defensive with Drones Outside & Alarms inside

156 **POST SHOW REPORT**
Highlights of Singapore International Cyber Week/ Govware 2017

BOSCH
Invented for life



They see a fun day of shopping.

You see smart data to help increase sales.

Bosch empowers you to build a safer and more secure world. And with built-in video analytics as of the IP 4000 cameras, we allow you to use video data for more than security alone. Anything from improving sales to increasing customer experience.

Find out more at **boschsecurity.com**

CONTACT

PUBLISHER
Steven Ooi (steven.ooi@tradelinkmedia.com.sg)

EDITOR
Melissa Teo (sst@tradelinkmedia.com.sg)

RADIO TECHNOLOGY CONSULTANT
Martin Gillmon (martin.gillmon@tradelinkmedia.com.sg)

GROUP MARKETING MANAGER
Eric Ooi (eric.ooi@tradelinkmedia.com.sg)

MARKETING MANAGER
Felix Ooi (felix.ooi@tradelinkmedia.com.sg)

MARKETING EXECUTIVE
Racheal Chong (racheal.chong@tradelinkmedia.com.sg)

HEAD OF GRAPHIC DEPT/ ADVERTISEMENT CO-ORDINATOR
Fawzeeah Yamin (fawzeeah@tradelinkmedia.com.sg)

GRAPHIC DESIGNER
Siti Nur Aishah (siti@tradelinkmedia.com.sg)

CIRCULATION
Yvonne Ooi (yvonne.ooi@tradelinkmedia.com.sg)

Photo Credit: Pixabay.com
Created by Harryarts - Freepik.com
Designed by Fawzeeah Yamin

SECURITY SOLUTIONS TODAY
is published bi-monthly by
Trade Link Media Pte Ltd (Co. Reg. No.: 199204277K)
101 Lorong 23, Geylang,
#06-04, Prosper House, Singapore 388399
Tel: +65 6842 2580 Fax: +65 6842 2581
ISSN 2345-7104 (Print)

Printed in Singapore by KHL Printing Co Pte Ltd.

ANNUAL SUBSCRIPTION:

Surface Mail:

Singapore	- S$45 (Reg No: M2-0108708-2 Incl. 7% GST)

Airmail:

Malaysia/Brunei	- S$90
Asia	- S$140
Japan, Australia, New Zealand	- S$170
America/Europe	- S$170
Middle East	- S$170

ADVERTISING SALES OFFICES

Head Office:
Trade Link Media Pte Ltd (Co. Reg. No: 199204277K)
101 Lorong 23, Geylang, #06-04, Prosper House,
Singapore 388399
Tel: +65 6842 2580 Fax: +65 6842 1523, 6846 8843, 6842 2581
Email (Mktg): info@tradelinkmedia.com.sg

China & Hong Kong
Iris Yuen
Room 1107G, Block A,
Galaxy Century Building
#3069 Cai Tian Road,
Futian District
Shenzhen
China
Tel : +86-138 0270 1367
sstchina86@gmail.com

Japan:
T Asoshina/Shizuka Kondo
Echo Japan Corporation
Grande Maison, Rm 303,
2-2, Kudan-Kita,1-chome,
Chiyoda-ku, Tokyo 102,
Japan
Tel: +81-3-32635065
Fax: +81-3-32342064

The magazine is available free-of-charge to applicants in the security industry who meet the publication's terms of control. For applicants who do not qualify for free subscription, copies will be made available, subject to the acceptance by the publisher, of a subscription fee which varies according to the country of residence of the potential subscriber in the manner shown on the right.

The editor reserves the right to omit, amend or alter any press release submitted for publication. The publisher and the editor are unable to accept any liability for errors or omissions that may occur, although every effort had been taken to ensure that the contents are correct at the time of going to press.

The editorial contents contributed by consultant editor, editor, interviewee and other contributors for this publication, do not, in any way, represent the views of or endorsed by the Publisher or the Management of Trade Link Media Pte Ltd. Thus, the Publisher or Management of Trade Link Media will not be accountable for any legal implications to any party or organisation.

Views and opinions expressed or implied in this magazine are contributors' and do not necessarily reflect those of Security Solutions Today and its staff. No portion of this publication may be reproduced in whole or in part without the written permission of the publisher.

Discover Checkpoint's
Protection @ Source
Look beyond the product !

SITE SURVEY AND PRODUCTION ANALYSIS

WIDE RANGE OF SOLUTIONS FOR ALL PRODUCT CATEGORIES

SOURCE TAGGING COMPLIANCE CERTIFICATE

AA AUTO APPLY SOLUTIONS

PROVEN ROI : -53% SCHRINKAGE

HIGH SPEED SOLUTIONS

VISIBLE SOURCE TAGGING

DEDICATED SOURCE TAGGING TEAM

BRIDGE TO RFID

3.500 PROTECTED REFERENCES

ANTI-DISCHARGE SOLUTIONS

ESD

DEVELOPING INTEGRATED SOLUTIONS WITH TECHNICAL PARTNERS

TUV MICROWAVE SAFE CERTIFICATION

ISEGA FOOD CERTIFICATION

TÜV Rheinland

20 YEARS EXPERIENCE

SOURCE TAGGING LAB

DEEP KNOWLEDGE OF INDUSTRIAL PRODUCTION

MORE THAN 600 VENDORS & 50 RETAILERS

Find out more at:

CheckpointSystems.com

Email: Apac.Marketing@checkpt.com

Checkpoint®

COMING SOON...

NOVEMBER 2017

ISC East 2017
Date: 15 - 16 Nov 2017
Venue: Javits Centre, New York City, USA
Organiser: Security Industry Association
Telephone: (800) 840-5602
Website: www.isceast.com
Email: inquiry@isc.reedexpo.com

NOVEMBER 2017

Secutech Thailand 2017
Date: 16 - 18 Nov 2017
Venue: Bangkok International Trade and Exhibition Centre, Bangkok, Thailand
Organiser: Messe Frankfurt
Telephone: +66 2 726 1999
Website: www.secutechthailand.tw.messefrankfurt.com
Email: jason.cheng@newera.messefrankfurt.com

DECEMBER 2017

IFSEC India 2017
Date: 6 - 8 December 2017
Venue: Pragati Maidan, New Delhi, India
Organiser: IFSEC
Telephone: +91 (0) 11 66517606
Website: www.ifsec.events/india
Email: pankaj.jain@ubm.com

JANUARY 2018

Intersec 2018
Date: 21 - 23 Jan 2018
Venue: Dubai International Convention and Exhibition Centre, Dubai
Organiser: Messe Frankfurt Middle East
Telephone: +971 4 389 4500
Website: www.intersecexpo.com
Email: andreas.rex@uae.messefrankfurt.com

SEPTEMBER 2018

Security Essen 2018
Date: 25 - 28 September 2018
Venue: MESSE ESSEN GmbH, Essen, Germany
Organiser: OTSA
Telephone: +49 (0)201 72 44-780
Website: www.security-essen.de
Email: www.security-essen.de

JUNE 2018

IFSEC 2018
Date: 19 - 21 June 2018
Venue: ExCel London, London, UK
Organiser: UBM
Telephone: +44 (0)20 7069 5000
Website: www.ifsec.events
Email: ifseccustomerservice@ubm.com

ARPIL 2018

ISC West 2018
Date: 11 - 13 April 2018
Venue: Sands Expo Center, Las Vegas, Nevada, USA
Organiser: Reed Exhibitions
Telephone: 2038405602
Website: www.iscwest.com
Email: inquiry@isc.reedexpo.com

MicroEngine®

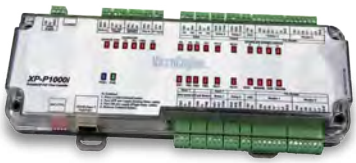
Integrated Security Systems

The Trusted Brand in Security Solutions

Plato DesFire Reader

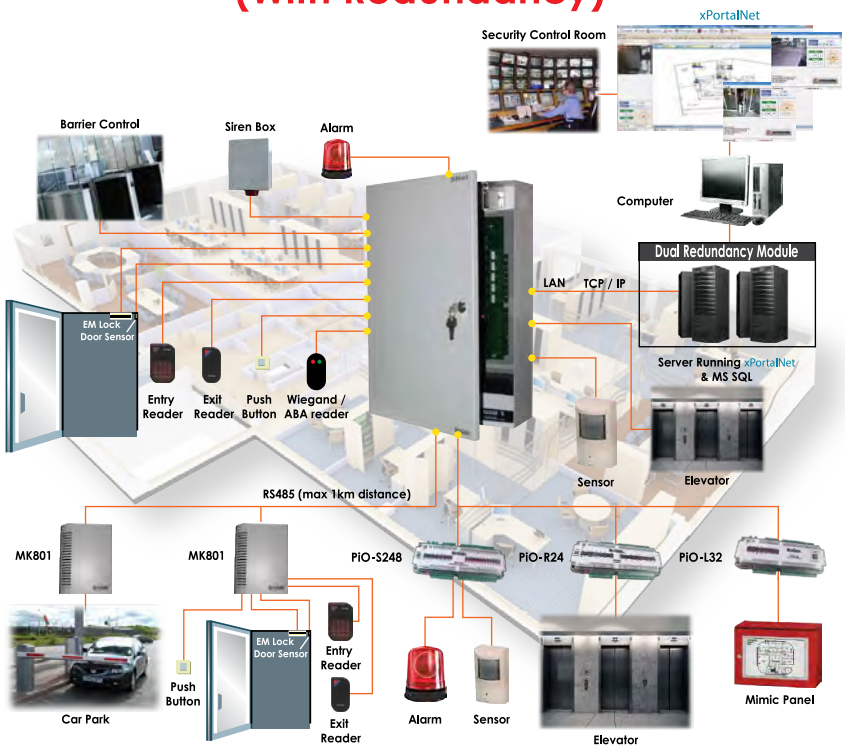
- 64 Bit Programmable Card ID
- Encrypted with 3DES
- Card ID Not by Serial Number

P1000i PoE Controller



- PoE with Battery Charger
- AES128 Encrypted IP
- Support 1 Door/2 Readers

Integrated Security System (With Redundancy)



Projects

Commercial / Complex | Factory | Condominium

Plato Reader - Slim Card Reader

500+ doors access & security system on SQL Server for factory and many more...

enquiry@microengine.net

www.microengine.net

Our Office

EDITOR'S NOTE

Dear esteemed readers,

We welcome you to our final issue for the year 2017 – our Nov/Dec edition of Security Solutions Today. We would like to thank you for your support and readership throughout the year as your publication developed along with the rest of the security industry. As always, it is with utmost pleasure that I present you with the latest trends, advancements and breaking news in the ever-evolving security sector. Join us as we explore the buzz in the SMART city, current events and much more.

In this issue, we explore the concept of security in SMART cities in greater depth. In our current connected age of the Internet of everything, criminal activity is shifting from the streets to the information super highway. The phenomenon of the world on WIFI has resulted in criminals becoming more and more sophisticated, which calls for law enforcement to stay abreast with the times. More than ever, police departments and other law enforcement agencies are focused on technological advancements in the security industries in order to enable them to fight crime the SMART way. From cyber security solutions to biometrics, artificial intelligence and even robotics, crime fighting has undergone a digital makeover in the quest to beat criminals at their own game. In the last two months alone, ransomware attacks have been on the rise along with cyber attacks carried out through connected devices with inadequate security measures in place. Online attacks have offline consequences resulting in real world catastrophes such as the malfunctioning of heart machines, electricity, transportation and more. In this issue, we present you with articles on the policing of SMART nations as well as the solutions currently being developed to assist law enforcement in safekeeping society.

Our Inside Look centres on the issue of public safety in SMART Cities. One consequence of digitisation is that criminals have become more sophisticated resulting in an increase in crimes such as data theft and blackmail. In order to deal with tech-savvy criminals, police officers have to be cyber vigilant at all times. However the solutions being offered to combat crime are influenced by government policies. As such, solutions will vary based on geographic location. Our Security Features in this issue comprise of an insightful collection of articles on the latest technological developments designed to meet the needs of flourishing cities of today such as security drones, wearable IoT devices and the migration of police databases to the cloud. On the surveillance front, we present you with the latest in CCTV tech including lip recognition cameras to pixel densities in IP cameras. Also included is an article addressing the issues faced in SMART cities and the measures undertaken by SMART law enforcement agencies to ensure public safety.

Having made its debut in the Sep-Oct issue of SST, Our connected world security section on IoT and Cyber security is back again with an exciting array of articles on the state of cyber readiness in Asia, Huawei's all new SMART video cloud solution, the launch of an endearing yet efficient SMART home security robot and much more.

In our In Focus section this issue, cyber vigilance takes centre stage as we sit down with 3 industry leaders in cyber security solutions – Dark Trace, Carbon Black and BAE Systems. Expert representatives from these remarkable organisations share their views on the alarming increase in cyber attacks via ransomware and hacking as well as ways in which both public and private sectors can work together to address high tech criminal activity.

Also included in this issue are informative titbits on police robots patrolling the world today as well as the futuristic face of crime prediction technology. Find out more on predictive policing and other SMART law enforcement solutions in my afterthought.

I certainly hope that you will enjoy this informative issue just as much as I have enjoyed curating it for your pleasure. 2017 has truly been an exciting time for the security sector, launching it from physical realm into the Internet of everything you could possibly think of. We most certainly look forward to bringing you more exhilarating developments in the year ahead as the industry goes digital with Artificial Intelligence, robotics, cyber biometrics and much more. The cloud is indeed the limit!

In conclusion, I would like to wish our readers Happy Holidays and Seasons Greetings to take you into a glorious 2018!

Melissa T
Editor

Everybody.

Everywhere.

Every day.

Ordinary days require extraordinary protection.

genetec.com

Find out more about the software behind the everyday at
genetec.com/protectingeveryday

Genetec™

© 2017 Genetec Inc. GENETEC and the GENETEC LOGO are trademarks of Genetec Inc., and may be registered or pending registration in several jurisdictions.

ABLOY UK at MLA Expo 2017

Security expert Abloy UK is showcasing its range of compliant security solutions at MLA Expo 2017, and highlighting the importance of fire and escape door standards in saving lives.

Shropshire, England, UK - Taking place at the International Centre, Telford, between 6th-8th October 2017, MLA Expo is Europe's largest exhibition trade show for the locksmith and security industry.

Products presented on Abloy's stand include a wide range of mechanical and electromechanical systems, some of which can be integrated with smart technology.

Standards expert Pat Jefferies will be hosting an interactive training session on compliance for escape and fire doors, and visitors to Abloy's stand H2.27 can also get a hands-on demonstration of the company's new products – eCLIQ and the Escape Door System (EDS).

eCLIQ is a completely electronic locking solution, which uses the mechanical precision and microelectronic modules of the PROTEC2 CLIQ system. The locks within the range are secure and reliable, with a compact waterproof design allowing for the strongest possible security.

The system also takes advantage of the core benefits of the PROTEC2 CLIQ solution, as each key is individually programmable. This solves the problem of lost keys and allows for access rights to be easily amended or deleted as required.

The EDS allows Read In / Read Out on Escape Doors without compromising safety or security, it complies with BS EN 13637 and it enables delayed egress as well as controlled egress with just a turn of the key.

Other products showcased on the stand include Abloy's range of compliant and energy efficient Electric Locks, EffEff Electric Strikes, Door Cylinders, Super Weatherproof Padlocks, Rim and Mortice Locks and Door Closers.

Pat Jefferies, Commercial Director at Abloy UK, "We know the MLA Expo is the key event in locksmith's diaries, and are keen to meet with visitors to discuss a range of topics including fire and escape door standards.

"Abloy not only has a wide range of compliant high security products, but we're also renowned for our expertise when it comes compliance and we're pleased to offer training on this and other topics at our Academy, to help make sure the right products are fitted in the right applications." SST

Abloy Celebrates 110 Years

Security expert Abloy is celebrating 110 years since the Finnish invention that sparked a revolution in the lock industry – founder Emil Henriksson's disc cylinder operated lock

Finland - With its unrivalled levels of product development, for over a century, Abloy has been at the forefront of the ever-changing global security market. Offering highly advanced and unique solutions, the Abloy name has become synonymous with quality and innovation.

This spirit of innovation began in Helsinki, in 1907 where precision mechanic Henrikkson recognised that the

continue on page 12

THE WORLD'S BIGGEST SECURITY TRADESHOW

28th YEAR CPSE - CHINA PUBLIC SECURITY EXPO

BPA WORLDWIDE

THE 16TH CHINA PUBLIC SECURITY EXPO

Oct 29-Nov 1, 2017 | Shenzhen Convention & Exhibition Center

The 14th China Public Security Forum

The CPSE Golden Excellence Award 2017

GSIA Gold Shield Award 2017

CPSE 2017 10/29-11/1 SHENZHEN CHINA

Exhibition Area (m²)	Exhibitors	Visitors	Booths
110,000	1,100	130,000	6,000

AIRONIX AXIS BOSCH Canon CHANGHONG CSST JXJ CNB alhua EverFocus FERMAX FUJICA HIKVISION

Honeywell H3C HUAWEI Infinova JinPeng JSST LG Panasonic Phenix Relong NATURE safer

SONY SIEMENS Skyworth SECOM Shidean Tiandy TAMRON tyco TCL VIDEOTREC WAPA Schneider WRT YAAN ZTE NetView

principle of the rotating detainer discs inside a cash register could be applied to locks. His initial idea for a secure and durable lock was patented in 1919, at which time, the now globally recognised Abloy trademark was also registered.

Thanks to its revolutionary disc design, the lock was virtually unpickable. This led to Abloy becoming the market leader in 1930's Finland and gaining momentum on a global scale, becoming the locking choice for some of the world's most important buildings.

The 1960's and 1970's saw the integration of electromechanical technology into Henrickkson's revolutionary mechanical lock and Abloy maintained its position as market leader during the rapid technological advancement of the following decades.

In 1994, Abloy merged with ASSA to form the ASSA ABLOY group. In the last decade, Abloy has developed game-changing access control systems such as PROTEC2 CLIQ™ and CLIQ Connect™, maximising security yet reducing the number of keys required.

Abloy's range of products encompasses mechanical and electric locks, as well as access control systems for applications including Utilities, Telecoms and Banking. Its innovative locking solutions can be found securing some of the world's most iconic landmarks from museums and sporting venues to hospitals, airports and government buildings.

Abloy continues to invest heavily in research and development to ensure that its product range consistently meets the changing needs of consumers, striving to offer not only what customers need, but what they will need in the future. Abloy remains proud of its roots and history, with each product maintaining Henriksson's Finnish values of reliability, resilience and durability. SST

LILIN and GJD Form Strategic Partnership to Accelerate North American Adoption of IP-Based Presence Detection

Arcadia, California, USA - LILIN Americas, an entity of Taiwan based IP video manufacturer Merit LILIN and UK based GJD Manufacturing Limited today announced a new joint initiative designed to accelerate the adoption of IP-based perimeter and intrusion detection technologies throughout the North American video surveillance sector.

The two industry-leading companies are teaming up to reduce false alarms common in standard motion detection sensors that occur while monitoring and illuminating large areas for intruders, while at the same time providing convenient, cost-effective compatibility with most major VMS and Home Automation Systems, including LILIN Surveillance, Mirasys Carbon, Milestone XProtect, Wavestore, Control4, Crestron and RTI.

As part of the agreement, LILIN will distribute GJD presence detection, LED illuminators and security lighting systems through its network of North American distributors. This step brings added depth to LILIN's already extensive portfolio of IP-based video products and gives its customers new technology that compliments the company's solutions.

"The addition of the GJD product line is an excellent fit for us," remarked Joe Cook, Vice President of LILIN Americas. "Our clients will have access to genuine GJD products and with the launch

continue on page 14

ATTEND secutech 2018 TO

EMBRACE

ICT, IoT and security technology trends

CompoSec: Key Components	ICT Transmission & LPWAN	Innovative Software: AI, IVA, edge computing & Big Data Analytics	IoT & Physical Cybersecurity

DISCOVER

State-of-the-art products

Video surveillance	Management software	Key components	Biometrics & RFID
Smart sensor	Transmission	Access control	Intrusion alarms
UAV	IoT security	Fleet management	Telematics & Automotive security

EXPLORE

Business opportunities in Intelligent Solutions Pavilions

Smart Factory	Smart Retail	Intelligent Transportation	Intelligent Healthcare	Mobility Asia

25–27 April 2018 | Taipei, Taiwan | **www.secutech.com**

of automation drivers, dealers will have an increased amount of solutions available for high-end applications in motion sensing and illumination with easy integration over IP using PoE."

Mark Tibbenham, Managing Director of GJD, said: "Teaming up with LILIN Americas is a great opportunity and honor for GJD. Our detectors and illuminators will sit alongside and interconnect with LILIN's world leading technologies making them readily available to LILIN's already extensive customer base and Custom Integrators."

Reducing false alarms

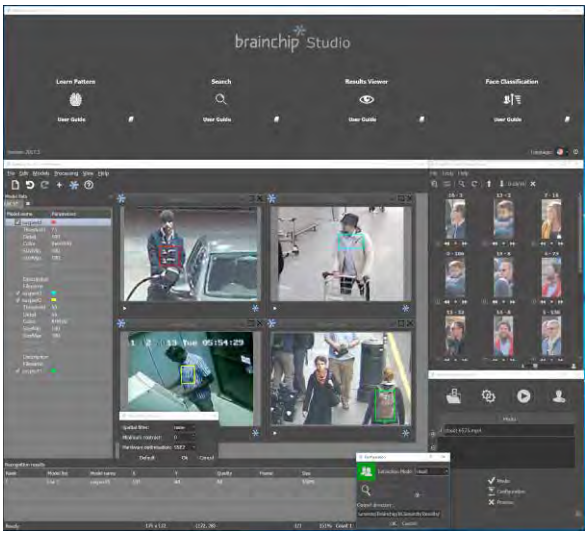
Even with advanced motion detection in place, false or nuisance alarms can be tripped by an event as simple as a change in the level of sunlight in the monitored area. False alarms needlessly waste the time, effort and money of on-site security or first responders when they must come to the scene.

GJD employs unique optical adjustment systems and programmable detection beam ranges to avoid false alarms caused by environmental factors and boundary overspill, giving advanced warning to security personnel of actual intrusion attempts so they have time to respond and protect the facility against theft, liability issues, attack or sabotage. GJD ensors precisely detect intrusion and greatly increase the effectiveness of onsite security, access control systems and video surveillance equipment. SST

BrainChip Studio Awarded New Product of the Year for Video Analytics by Security Today's Panel of Independent Judges

AI-powered software is easily deployed in existing infrastructure, where it rapidly searches archived video or live streams to identify objects or faces

Aliso Viejo, California – BrainChip Holdings Ltd , a leading developer of software and hardware accelerated solutions for advanced artificial intelligence (AI) and machine learning applications, has won the Security Today's New Product of the Year Award 2017 in the Video Analytics category for its BrainChip Studio software suite. The award honors the outstanding products considered to be particularly noteworthy in their ability to improve security. The trophy will be accepted by BrainChip during the ASIS International 63rd Annual Seminar and Exhibits, September 25th – 28th, Dallas, Texas.



BrainChip Studio aids law enforcement and intelligence agencies to search vast amounts of video footage many times faster than previously possible, enabling them to quickly identify patterns or faces. Most significantly, the software can be utilized with existing infrastructure.

The software suite simulates the spiking neural networks found in the human brain. It works with low-resolution video, even in noisy environments, and requires only a 24x24 pixel image to detect and classify faces and objects. Furthermore, BrainChip Studio can be trained on a single image in milliseconds and does not need the vast datasets, extended learning time or substantial compute power associated with other forms of video processing using artificial intelligence.

Now in its ninth year, Security Today's New Product of the Year Award is selected at the sole discretion of an independent panel of judges from the security industry.

continue on page 16

2018 SECURITY CHINA

the 14th China International Exhibition on Public Safety and Security 2018

New China International Exhibition Center

Beijing China

October 23 - 26. 2018

Wechat: cspmag

Wechat: securitychina

Approved by:
the Ministry of Public Security of the People's Republic of China
the Ministry of Commerce of the People's Republic of China

Organizer:
China Security and Protection Industry Association

www.securitychina.com.cn

"At a time of heightened global security, BrainChip Studio meets the urgent need for a rapidly deployable object and facial search technology to tame the massive volume of video footage already created and in the making," said Bob Beachler, BrainChip's SVP of Marketing and Business Development. "We are extremely honored to receive the Security Today New Product of The Year Award, which validates the groundbreaking nature of BrainChip's technology."

BrainChip Studio software runs under Windows or Linux. It is compatible with all major video encoding formats and is available to select law enforcement and intelligence agencies. SST

NTT Communications Addresses Top Internet Trends: More Businesses Defending Against Cyberattacks, Surging Demand for OTT Video, Faster Data on the 'Edge'

Growing Number of Businesses Have Cyberattack Response Plan In-Place, Surging Popularity of OTT Driving Need for PoP Installations in Smaller Markets

New York, USA - Record numbers of consumers are going online for commerce, news and OTT video entertainment and that's making the world's top Internet-centric businesses and organisations increasingly motivated to defend themselves against cyberattacks that can disrupt customer access. These are some of the top line industry assessments provided today by NTT Communications Corp. (NTT Com), a company that owns and operates one of the world's largest IP backbones and is the data and global IP service arm of Fortune 500 telecom leader NTT.

More Businesses Taking a Proactive Approach to Network Security

"Through the first half of 2017 we're seeing an increased demand for network security – especially for services that allow for more proactive and robust defenses against DDoS attacks," said Michael Wheeler, executive vice president of NTT Communications Global IP Network at NTT America. "In previous years, many businesses and organisations viewed these types of protections as 'optional' where, today, they are viewed as 'must haves'."

According to NTT Security, more than six billion cyberattacks were attempted in 2016 on client networks across six continents. Cisco also reports that DDoS attacks grew by 172 percent that same year and many industry analysts expect they will continue to grow in frequency, size and complexity. This reality is forcing a lot of businesses to re-assess their ability to pre-empt as well as respond to increasingly sophisticated attacks – including ones that target Internet of Things (IoT) devices that can be especially vulnerable.

"With the number of cyberattacks continuing to grow, our research shows that more than one-third of businesses and organisations around the world have assembled formal incident response plans," added Wheeler. "We anticipate that this will increase dramatically in the year ahead."

NTT Com recently announced the expansion of its DDoS Protection Services, offering Global IP Network customers the opportunity to choose the tier of support they need based on their own cyber defense strategies and plans.

OTT Video Reaching the Mainstream, Will

continue on page 17

Dominate Internet Traffic

Over-the-Top (OTT) video providers including Netflix, Hulu and Amazon Prime are surging in popularity with half of U.S. broadband subscribers paying for at least one OTT video service and 30 percent paying for two or more, according to a recent report by IBB Consulting.

"OTT video will continue to grow in popularity and we believe that both video on demand (VOD) and live streaming will dominate Internet traffic in years to come," said Wheeler. "And while many carriers might see OTT providers as adversaries, the relationships will most likely be mutually beneficial in the long term as OTT video transmissions and massive amounts of data are large contributors of network growth."

Better User Experiences for Consumers and Businesses on 'the Edge'

While most major markets around the world are close to large scale Point of Presence (PoP) and data center installations that ensure fast and efficient delivery of data, many businesses and consumers in tier-2 and -3 markets are further away.

"If data only resides in big tier-1 markets, there are hundreds of millions of users around the world that are far away from that data," said Wheeler. "This is particularly important in Latin America, Asia and Africa. If all the data in Asia was stored in Japan, Hong Kong and Singapore, the negative impact on accessibility, latency and efficiency for consumers would be significant."

To avoid delays, many global corporations – especially Internet-centric businesses in areas such as e-commerce, gaming, social media and OTT – and even large-scale government agencies are setting-up installations closer to the edge. Even in the U.S., some of the large colocation companies are setting up facilities outside the traditional, larger markets. This proliferation of data sitting on the edge enhances consumer experience and results in higher utilisation of the services, benefiting everyone involved in the Internet ecosystem. SST

CrowdStrike Expands Operations in APAC and Achieves Strong Growth in First Half of 2017

Company broadens footprint in Singapore, New Zealand, India and Northern Asia; appoints key hires in Asia Pacific Region

Sydney, Australia - CrowdStrike® Inc., the leader in cloud-delivered endpoint protection, today announced the rapid expansion of its Asia Pacific (APAC) operations on the heels of triple-digit bookings growth. The company has established offices and headcount in key markets including Singapore, New Zealand, India and Northern Asia. Increased demand within the APAC region for CrowdStrike Falcon®, the first cloud-based endpoint protection platform, continues to spike as organizations replace legacy antivirus (AV) solutions with next-generation technology.

CrowdStrike Falcon is the only platform that unifies next-generation AV, endpoint detection and response (EDR), and a 24/7 threat hunting service all delivered via a single lightweight agent. With CrowdStrike Falcon, organisations can replace their AV or augment it with a full-scale endpoint protection solution, powered by a cloud-native architecture and artificial intelligence/machine learning.

While CrowdStrike opened APAC headquarters in June 2016, the organisation has had customers within the region for more than four years. Since then, CrowdStrike has seen growing momentum in its business and operations, sales growth, and a rapidly expanding customer base. This May, CrowdStrike completed a $100 million Series D funding round, led by existing investor Accel along with CapitalG (formerly Google Capital), Warburg Pincus, March Capital Partners and regional investor Telstra. This round of funding will help CrowdStrike further accelerate its APAC expansion to meet the spiking demand for its Falcon platform.

In tandem with expanding operations, CrowdStrike has made multiple strategic hires to continue investment in the APAC region including regional director for India and SAARC, APAC director of Channel and Alliances, and regional Sales and Marketing managers for New Zealand, Southeast Asia and Victoria, Australia. CrowdStrike's operations in APAC now include Australia, New Zealand, Singapore, India, and parts of Northern Asia.

Other regional milestones include:

- 245 percent growth in new customers, year over year
- Total bookings year-over-year increased by 410 percent
- 154 percent channel pipeline growth
- Doubled headcount and continued investments to broaden the partner and channel pipeline

Kevin O'Sullivan, head of Security Services, Kinetic IT was quoted as saying that today, customers are looking to move away from point products and adopt comprehensive solutions to not only transform their legacy AV but also add capabilities to detect and respond to advanced attacks. CrowdStrike Falcon offers exactly that and enables customers to stop breaches regardless of how threats continue to evolve. CrowdStrike and Kinetic IT share a commitment to putting the customer first and delivering best-of-breed solutions to drive value and ROI and we look forward to continuing to our productive partnership.

"As a global, next-gen cybersecurity services provider, Proficio is continually focused on providing its clients with state-of-the-art monitoring, detection and response solutions like CrowdStrike's Falcon platform. Through our valued partnership with CrowdStrike, we are able to offer our clients the most comprehensive and effective solution to stop modern-day attacks and give them a definitive advantage against the rising tide of threats that they are facing not just in the APAC region but globally as well. The CrowdStrike Falcon platform not only improves our overall visibility into our customers' environment but also allows us to provide better actionable intelligence, recommendations and remediation", said Michael Ostrowski, regional Vice President of Sales, APAC at Proficio. SST

Genetec Announces New Access Control as a Service Offering

Security Center Synergis to be available in a Software as a Service (SaaS) edition; will deliver greater accessibility, convenience, and easier maintenance via the cloud

Montréal, Canada — Genetec Inc., a leading technology provider of unified security, public safety, operations, and business intelligence solutions, today announced Security Center Synergis™ SaaS edition. This new edition will offer a turnkey access control solution for easier deployment and maintenance. Synergis SaaS edition removes the need to purchase and install costly on-premises servers and streamlines maintenance, allowing the corporate IT staff to focus on other business-critical projects. Synergis SaaS edition is expected to be available in November 2017, and will be demonstrated at ASIS 2017 (booth #3147).

Synergis is the access control solution in Genetec Security Center, an open-architecture, IP security platform that combines video surveillance, access control, automatic license plate recognition (ALPR), communications, and analytics. All Synergis access control software editions integrate with a wide selection of access control hardware from leading manufacturers.

The new Synergis SaaS edition will give customers the flexibility to adjust their system usage as their needs change, reducing budget requirements for access control capital expenditures. Customers will also be able to quickly and efficiently deploy their access control system, and benefit from automated update notifications. Multi-site organisations will be able to centrally manage their access control systems more efficiently.

"When we introduced Synergis™ Cloud Link a few years ago, our forward-looking strategy was to offer a future-proof gateway appliance that is cloud-ready," said Derek Arcuri, Product Marketing Manager for Access Control, Genetec Inc. "Today, we take great pride in announcing Synergis SaaS edition, which will allow customers to leverage all the benefits of Access Control as a service (ACaaS), as they renew their legacy access control systems, while retaining elements of their existing infrastructure," added Arcuri.

For more information, please visit: www.genetec.com SST

Kentec Helps Protect Joburg Bank

Johannesburg, South Africa - A new life safety system based around Kentec's market leading control panel technology is protecting a major Barclays Bank installation.

The new fire safety system, supplied and installed by SFP Security & Fire (Pty) Ltd., in an L1 system configuration includes a new network of four Kentec Syncro AS analogue addressable fire control panels. The open protocol system has Apollo analogue Series 65 devices and call points installed.

In areas such as Server/Data Rooms, MV and LV rooms, Generator and Diesel Tank rooms, existing extinguishant protection has been extended with the addition of five Sigma XT+ Extinguishing Control Panels to the existing network of fifteen Sigma XT Panels. The extinguishing control panels are being monitored by the four Kentec Syncro AS analogue addressable fire control panels through multiple three channel interface units, which form part of the addressable building detection loops.

Kentec's Sigma XT Extinguishing Control Panel range is designed to comply with the requirements of EN12094-1, EN54-2 & EN54-4. It features 3 detection zones as standard, where any zone or any combination of zones can be configured to release the extinguishant gas and allows delay in first stage sounder and detection to be configured, with an instant release facility by using the manual release option. The Kentec Sigma XT is compatible with Intrinsically Safe barriers, which makes it ideal for use in hazardous areas.

Kentec, leaders in extinguishant technology since 1985, were the first company to introduce an EN12094-1:2003 compliant extinguishing panel and were able to apply the CE mark showing compliance with the Construction Products Directive to any type of fire control panel. SST

Johnson Controls Releases Extended Fire Alarm Control Panel Range

Enhanced ZETTLER PROFILE range

Milwaukee, USA – Johnson Controls is pleased to launched its innovative PROFILE Flexible range of modular fire alarm control panels. Enhancing its existing ZETTLER PROFILE range, Johnson Controls has developed the new panels to provide advanced flexibility and usability, ease of installation and significant cost saving benefits.

The new range of PROFILE Flexible panels contain a slot card mechanism which allows it to be tailored to specific end user needs, by offering approximately 50 different options to build the most economical system. To reduce the total cost of ownership, PROFILE Flexible panels contain backwards and forwards compatibility, which ensures that they can be easily integrated with fire panels that use ZETTLER's MZX fire detection technology platform. This makes upgrading from existing systems efficient and cost effective.

These panels provide increased loop power to meet the demand for visual alarms as well as traditional audible alarms. With one amp of power per loop, system designers can allocate 250 addresses to a single high power loop, or share resources across two shared power

continue on page 22

IFSEC International

SECURING PEOPLE, PROPERTY & ASSETS

19-21 JUNE 2018 EXCEL LONDON UK

> "You have to be here if you want to be regarded as a key player in the security market."

27,658
visitors from 116 countries

79%
of visitors come to source new products

£20.7bn
total budget of visitors to IFSEC 2017

Enquire about exhibiting at IFSEC 2018: **ifsec.events/international**

Proud to be supported by:

ASIS INTERNATIONAL · bre · bsia · IPSA · LONDON FIRST · LPCB · NSI · SSAIB

loops. This level of optimisation can significantly reduce total system installation costs.

Users can also combine the high powered and shared powered loops to enable their system to be designed in line with the layout of their building. This maximises loop power usage and prevents wastage. PROFILE Flexible panels have the capacity to support 4000 addresses per panel and up to 99 panels per network, which makes it possible to expand the system and further reduces the total system installation cost, as additional panels do not need to be installed. When a business' requirements change, the capabilities of PROFILE Flexible panels can be expanded through the slot card mechanism and future upgrades can be managed.

Another key benefit of this new range is user operability. PROFILE Flexible panels offer a multilingual touchscreen user interface with touch sensitive status LEDs. These have been ergonomically engineered to facilitate ease of operation, as users can access event summary information in just one tap. Operation of the touch screen is possible with or without gloves, meaning the systems can be used in a wide range of environments.

Stephen Bennett, Senior Global Product Manager for ZETTLER Fire Detection, said: "As technology revolutionises the construction industry, buildings are now smarter, providing greater flexibility to occupants based on their needs. As a world leader in the design and manufacture of fire detection products, Johnson Controls has built a control panel for the future that will evolve alongside building design requirements.

"The new PROFILE Flexible range combines high performance with ease of use, and its innovative features bring lifetime cost benefits to end users. The systems are easy to install, configure and use and they provide the system designer with a wide range of practical engineering solutions.

"Highly resistant to electrical noise and common false alarm triggers, the PROFILE control panels can operate effectively in the harshest of environments. However, they are equally suited to aesthetically pleasing environments through their state-of-the-art design and mounting options. Its level of flexibility and range of customisable features makes the PROFILE Flexible range a valuable long-term investment." SST

Malwarebytes Introduces Malwarebytes for Mac to Protect Against Rising Levels of Mac Malware

- *Mac users saw more malware in Q2 (April to June) than they saw in all of 2016*
- *Malwarebytes now provides real-time cyber protection for Mac users*

Santa Clara, California, USA – Malwarebytes , the leader in advanced malware prevention and remediation solutions, today announced the release of Malwarebytes for Mac, featuring real-time protection to automatically block and remove cyber threats, including malware, adware and potentially unwanted programs. The innovative and fast detection engine has minimal impact on device operations to ensure Mac computers run like they should, and is recommended over traditional antivirus programs by many professionals.

According to data collected by Malwarebytes, Mac users saw more malware in the second quarter (May to June) than they had seen in all of 2016. In fact, more new malware families have appeared this year than in any other previous year in Mac history.

"We carefully designed Malwarebytes for Mac to protect all Mac users from cyber threats and potentially unwanted programs so that they can feel safe and have a Mac that performs like it should," said Marcin Kleczynski, CEO, Malwarebytes. "Antivirus and security awareness is no longer enough defense for Mac users, the growth of Mac malware has made that very clear. We hope that more and more Mac users will come to this realisation and begin to seek out additional defenses."

continue on page 23

Malwarebytes for Mac features several distinct benefits and features for users to protect against this increasingly dangerous Mac threat landscape, including:

- Real-time Anti-Malware Protection Scanner: Malwarebytes for Mac provides ultra-fast proactive scanning for malware and spyware in real-time, in addition to flagging potentially unwanted programs and adware
- Antivirus Replacement or Complement: Malwarebytes for Mac completely replaces existing antivirus solutions or can run alongside any antivirus program
- Small System Footprint: Malwarebytes for Mac utilizes minimal system resources to ensure that Macs run smoothly

Malwarebytes for Mac is highly recommended by technicians as a primary defense against the growing threat of Mac malware. "As the top Apple Tutorialist on YouTube, Malwarebytes for Mac is one of very few pieces of software that I recommend to ALL Mac users," said David A. Cox, CEO, Tech Talk America.

"Mac threats are not taken seriously enough in the security community today," said Thomas Reed, Director of Mac and Mobile, Malwarebytes. "Adware and potentially unwanted programs are becoming a major problem for Mac users. Some very popular apps have been known to carry these threats and despite protections in place, the App Store is not immune to these threats. For example, the recent Proton Remote Access Trojan that plagued Mac users fooled many experienced, security-minded people who became infected. This perpetuates a crucial lesson that, despite what many Mac users think, they are not safe even if they are careful about what they download. Being security-savvy is no longer enough, all Mac users need dedicated protection against malware, adware and potentially unwanted programs." SST

Avigilon Appearance Search Video Analytics Technology Winner of Benchmark Innovation Awards 2017

Avigilon recognised as an industry leader in artificial intelligence-driven video analytics

Vancouver, Canada - Avigilon Corporation, provider of trusted security solutions, today announced that Avigilon Appearance Search technology has been selected as the winner of the Intelligent Systems category in the Benchmark Innovation Awards 2017.

The Benchmark Innovation Awards is an annual showcase that recognises and rewards innovative thinking and the delivery of benefits through advanced security solutions.

Winning in the Intelligent Systems category, Avigilon Appearance Search is Avigilon's newest and most advanced video analytics technology. It is a sophisticated deep learning artificial intelligence (AI) search engine that sorts through hours of footage with ease, allowing users to quickly locate a specific person or vehicle of interest across all cameras on an entire site. It can save time and effort during critical investigations as it intelligently analyzes large volumes of video data in seconds, helping to track a person's or vehicle's route and identify previous and last-known locations.

"Avigilon's commitment to innovation and developing deep learning AI technology is taking video analytics to new levels," said Dr. Mahesh Saptharishi, Avigilon's Chief Technology Officer. "We are honored that Avigilon Appearance Search has received this award and we continue to focus on introducing new video analytics technology to change how users interact with security systems." SST

BT Selects Sydney for Global Cyber Security Hub Expansion

The hub will tap into local talent pool to develop new cyber security services for global customers

New South Wales, Australia - BT and New South Wales Government today announced the opening of a new global cyber security research and development hub in Sydney. The hub is an expansion of BT's existing Security Operation Centre (SOC) and will create up to 172 new highly skilled jobs over five years, further cementing New South Wales as Australia's cyber security hotspot.

The hub is BT's first cyber security R&D facility outside of the United Kingdom and will employ highly qualified cyber security specialists. The areas of expertise in the new hub will include cyber security, machine learning, data science analytics and visualisation, big data engineering, cloud computing, data networking, and the full life cycle of software engineering. The centre will also offer job opportunities for 38 graduates with relevant degrees.

The expanded operations centre and R&D hub is part of BT's global network of 14 Security Operations Centres, providing cyber security service for global customers in 180 countries around the world. BT is recognised by industry analysts as one of the world's leaders in managed security services on a global level as well as in the Asia Pacific region specifically.

Security solutions developed and supported out of the Sydney hub will be deployed for customers locally and globally. The hub will also host cyber security systems integration and services teams as well as BT's newly created role of chief global engineer for cyber product development.

Minister for Innovation Matt Kean said the NSW Government-backed Jobs for NSW would provide a $1.67 million grant to BT.

"This cutting edge operation will help keep Australia's best cyber security talent here in NSW while nurturing our next generation of specialists to ensure we remain a regional leader in this fast growing industry.

"As well as creating 172 jobs, including 38 jobs for skilled graduates over the next five years, BT will also make a $2 million investment in capital infrastructure and a further multi-million dollar investment to employ cyber security specialists at the hub."

Mark Hughes, CEO BT Security, said: "We are thrilled at this exciting new opportunity to tap into local cyber security skills. Never before has cyber security been more important and we see potential for growth in New South Wales, Australia and further afield. The hub will be a cornerstone of our global cyber security capabilities and help us stay ahead in this fast moving space." SST

OMVS: Robotic Assistance Devices Announces Strategic Partnership With Romeo Power Will Deploy Two Robots

Reno, Nevada, USA - On the Move Systems is pleased to announce that Robotic Assistance Devices has entered into an agreement with Romeo Power to outfit the SMP Robotics S5 Security Guard Robot with Romeo's lithium-ion energy solution. RAD will exclusively use Romeo's power solution and similarly Romeo will only supply RAD as their exclusive security robot partner. The addition of Romeo's battery packs to the RAD robotics solution delivers 12 hours of continuous operation regardless of terrain or climate. Romeo Power's advanced battery packs also allows four continuous years of use without replacement.

continue on page 25

"This advanced battery from Romeo allows our autonomous security robot to patrol for longer periods of time, increasing its efficiency and operational success. As we gear up to deploy more advanced robotic solutions to the market, the battery life and power will be a critical feature we can offer to end users," said Steve Reinharz, President and Founder, RAD. "Additionally, Romeo Power is an ideal technology partner as it leads the charge in developing power solutions that drives today's modern technology deployments."

As part of the company's alliance, Romeo Power will deploy two S5 autonomous security guard robots at its Vernon, Calif., headquarters, to patrol its 113,000-square-foot manufacturing facility and the surrounding property.

"We are excited to have the opportunity to leverage RAD robotics to help increase safety, enhance productivity and control access to our facility," said Michael Patterson, CEO and Founder, Romeo Power. "Furthermore, our partnership with RAD will allow us to further refine the lithium-ion battery for use within the artificial intelligence market, which is expanding at a rapid rate."

Romeo Power, founded by engineers and designers from SpaceX, Tesla, Samsung, and Amazon, focuses on battery pack innovation, safety and reliability for manned and unmanned vehicles, and personal power products.

RAD has commenced to deploy robots to end users. To date RAD has commitments for 62 robots for total contract values of approximately $6 million. OMVS has successfully completed its due diligence process on RAD as part of the binding LOI that was entered into on May 10th, 2017 for the purchase of 100% of RAD by OMVS. It is anticipated that the acquisition will close before August 31, 2017.

RAD currently has signed agreements for 2 POC's with major companies.

RAD currently has a sales pipeline of over 50 Fortune 500 companies and over 25 qualified dealers and distributors that have a combined customer base of more than 35,000 end user corporations. SST

Panama City's Golden Lion Marbella Casino Selects Qognify's VisionHub

One of the city's largest and best known casinos chooses VisionHub to improve security and safety

Pearl River, New York, USA – Qognify, the leader in big data solutions for physical security and operations, today announced that Golden Lion Marbella, one of Panama's top-ranking casinos, has selected Qognify VisionHub to upgrade security, safety and operations. Formerly the Princess Casino Marbella, Golden Lion features one of the largest casinos in Panama City which will now enjoy total coverage with Qognify's security solution for gaming featuring its market leading VMS, VisionHub.

The casino environment is an enticing target for criminal behavior for both

continue on page 26

visitors and employees – with large amounts of money constantly changing hands. Continuous, reliable 24x7x365 monitoring is a necessity for theft and fraud prevention, allowing casino security management to identify, verify and resolve unfolding incidents. VisionHub provides 100% system availability combined with high-definition video quality casinos need when monitoring card playing and money counting.

The security program at the casino serves as both a deterrent and accurate, non-refutable method to settle disputes. "VisionHub gives us the ability to view gaming sequences from many different angles and zoom in for close-ups," said Mr. Hasky, President of Sortis Hotel, Spa & Casino, Golden Lion Marbella. "If a dispute arises, we can scroll through the video quickly – back and forth – and view images from several cameras simultaneously. We can see the fine details, which cards each player held, the exact amount of a bet and when it was placed."

Specific industry experience is particularly important in the gaming industry. "Gaming is a challenging environment that requires an exceptional enterprise solution," said Moti Shabtai, CEO and President of Qognify. "The solution our teams designed for Golden Lion Marbella enables them to cost-effectively monitor the entire casino operation, with high-quality video. In turn, this facilitates the prevention of potential security issues, promotes the safety of guests and protects the integrity of casino operations." SST

Rapiscan Chosen to Provide Security Screening Systems for the 2018 Gold Coast Commonwealth Games

Queensland, Australia - Rapiscan Systems, a leading global supplier of security inspection systems, is pleased to announce that the Gold Coast 2018 Commonwealth Games Corporation (GOLDOC) has chosen us as their security screening equipment provider. With 6,500 athletes and thousands of spectators expected to participate over the 11 day competition, GOLDOC welcomes Rapiscan's major event security experience.

Rapiscan has longstanding, global experience in providing total security solutions for major sporting events worldwide; including at the Glasgow 2014 Commonwealth Games, and the London 2012 Olympic Games.

OSI Systems (Rapiscan Systems' parent company) CEO, Deepak Chopra, commented, "We are proud to be chosen for this prestigious international sporting event to help ensure the safety of athletes and spectators. Our total security solutions and unparalleled event security experience are an ideal fit for securing multi-day competitions at large venues."

Rapiscan will provide several products for checkpoint security including its Rapiscan® 600 Series Baggage and Parcel Inspection systems, Metor® Metal Detectors and Detectra® Explosives Trace Detection systems to help secure numerous entry points at the Games. Designed for rapid relocation and easy deployment, Rapiscan inspection systems are ideal for large venues with numerous points of entry. SST

continue on page 27

VTT to Develop Intelligent Transport Systems in Cooperation with ITS Russia

Finland - VTT Technical Research Centre of Finland Ltd and ITS Russia have signed a partnership agreement concerning the development of intelligent transport systems (ITS). The objective of Project CAVLANE is to develop new services, products and standards for border crossings in particular. Businesses from all over Europe are hoped to join the partnership.

CAVLANE is linked to an initiative of the Russian Ministry of Industry and Trade to create a roadmap for transport solutions that support automated driving as well as to the Autonet-2 scientific and technical initiative. "The goal is to promote automated driving and therefore to prepare for the advent of robotic cars with varying degrees of autonomy. VTT has a long history of developing the reliability and safety of autonomous cars", says Executive Vice President, Erja Turunen from VTT.

New intelligent services increase road safety, improve logistics, boost businesses' competitiveness and create markets for new innovations. The project involves, for example, testing ITS services for drivers before and after border crossings, such as queue cautions that are hoped to make traffic flow more smoothly at the Nuijamaa border crossing point and standardised EU V2V warning messages.

New Partnerships and Business Opportunities

Project CAVLANE has already helped to network a host of Finnish organisations and businesses. VTT is in charge of coordinating the national business consortium, which currently consists of Indagon, Nokia, Vediafi, Dynniq and Infotripla. "We are looking for Finnish businesses in particular to join the partnership, but we also welcome ITS expert from other countries", says Project Manager Lasse Nykänen from VTT. There is also a similar business consortium in Russia, which is coordinated by ITS Russia.

The Finnish Transport Safety Agency's TrafficLab and the Finnish Ministry of Transport and Communications launched a project aimed at enabling new transport services for cross-border transport in May. "The starting point is to promote cross-border cooperation with Russia or other Nordic countries. The aim is to begin testing new transport services through a business-led approach", explains Director General of Data and Knowledge Juha Kenraali from the Finnish Transport Safety Agency. VTT is also in charge of a project launched by TrafficLab in May, which involves testing digital transport services in arctic conditions and offering seed money to businesses.

"Automated driving, which will become a reality at the beginning of the next decade, has turned smart mobility solutions and services into a growth industry. Our role in the project is to test new intelligent, accurate and reliable online driver assistance systems, as the business around these kinds of devices is growing at a rate of more than six per cent per year globally", explains CEO Matti Lankinen from Indagon Ltd.

Finland as an ITS Gateway to China

The aim is to link CAVLANE to an ITS route sponsored by the Russian Government, which would begin from the biggest cities in Finland and run via Helsinki to Saint Petersburg, Moscow, Kazan and China.

"Building an ITS and logistics route from Finland via Russia to the Far East is extremely important both economically and in terms of transport, and we want to promote its implementation together with businesses and various stakeholders. At its best, the route can act as a platform for collaboration that benefits everyone involved in the global transport and logistics revolution", says Senior Adviser Seppo Öörni from the Finnish Ministry of Transport and Communications. SST

Forcepoint Simplifies Cybersecurity Through Cloud-Based Behavior Analytics

- *New Forcepoint CASB behavior analytics help enterprise and government security teams reduce time to action by focusing on the business impact of highest risk users*
- *Forcepoint Web Security and Forcepoint Email Security deliver new cloud application controls and Advanced Malware Detection service enabling rapid, secure cloud adoption and management*

Singapore – Global cybersecurity leader Forcepoint today fortified its cloud security portfolio to empower security teams with new behavior-driven controls that simplify protection of employees, critical business data and intellectual property (IP). New capabilities now available across Forcepoint CASB, Forcepoint Web Security and Forcepoint Email Security ensure customers around the world can safely embrace, and continue to grow, their business in the cloud.

According to Gartner, the average time to detect a breach is 99 days with an average cost of $4 millioni; however, enterprises can shorten dwell time utilising data and analytics. The firm expects by 2018 80 percent of endpoint protection platforms will include user activity monitoring and forensic capabilities — up from less than 5 percent in 2013ii, and estimates at least 25 percent of self-discovered enterprise breaches will be found using user and entity behavior analyticsiii.

"Approaching security through a human-centric lens helps organisations better understand indicators of normal cyber behavior and quickly identify activity and operations, such as shadow IT, that pose the biggest risk," said Kris Lamb, vice president and general manager of the Cloud Security business at Forcepoint. "As enterprises and government agencies shift their applications to SaaS and cloud IT models, they require intelligent systems that quickly spot anomalies, assess risk and facilitate rapid resolution to protect users and their data in an increasingly zero perimeter world."

Enabling cloud-first security strategies

Forcepoint is delivering today new CASB capabilities that assess the risk posed by file sharing and other cloud applications and protect against the loss of critical business data and IP not stored on a corporate network. Forcepoint CASB now analyses user behavior and characteristics of the application, such as the data, device and location being accessed. A new single-view User Risk Dashboard reports both employee behavior and, unique to Forcepoint CASB, the potential business impact based on the user's account permissions within an organisation. Security teams can now access actionable insights faster with a full understanding of risk at-a-glance; and, when CASB is used with Forcepoint Advanced Malware Detection powered by Lastline, organisations can be assured their data is fully protected from both risky users and malware posing as a user.

Real-world threats facing enterprises and government agencies today can be thwarted through Forcepoint CASB behavior analytics. For example, banks transitioning from delivering on-premises to cloud-based financial services and infrastructure require protection for employees using Microsoft Office 365 as well as contract developers using Amazon or Azure public clouds to develop custom applications. In healthcare, departing physicians downloading patient files from their electronic health records (EHR) system to personal cloud storage for use in a new practice will raise their user risk ranking and enable quick response by the security team to revoke access and stop the attempted data export.

Forcepoint further enhanced its Forcepoint Web Security and Forcepoint Email Security cloud and on-premises offerings today with new features and tools, including; Forcepoint Web Security enhancements enable more granular control of cloud applications and blocking unsanctioned shadow IT.

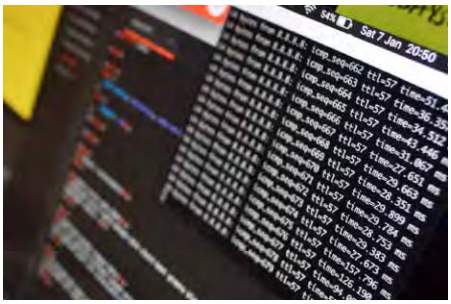
Forcepoint Web Security with new cloud migration tools to Forcepoint Web Security Cloud help on-premises appliance customers migrate when ready.

Advanced Malware Detection (AMD) Powered by Lastline is now available for on-premises and cloud Forcepoint Web Security and Forcepoint Email Security platforms. Integration of AMD sandbox technology enables real-time protection of users anywhere. SST

continue on page 29

In the Times of Fortnightly Attacks, Singapore Hosts an Elite Gathering of Fintech and Cyber Security Experts

Singapore - EC-Council announced the launch of the Fintech Security Summit, Singapore on the 25th August 2017 at Shangri-La Hotel, Singapore.
Digitally, Singapore is one of the most connected nations in the world. As more financial services go online, there is a large risk of attacks surfacing due to connected endpoints.



Owing to these alarming cyber security issues, EC-Council brought together 30+ experts, 120+ C-Suite delegates from public sector, banking and financial services, fintech and many more to expand their understanding of how to infuse security awareness into everyday culture and strategies to help people evolve their cyber resilience.

Along with Wissen and Quann Asia Pacific, EC-Council proudly presented an exclusive Certified Chief Information Security Officer class which was scheduled for 4 days preceding the Summit, from 21st to 24th August, 2017. e2i supported this workshop to enable ICT professionals to benefit from this opportunity.
Some of the eminent industry speakers are:

- Boon Hui Khoo - Commissioner, Global Commission for the Stability of Cyberspace
- Michael Gorriz - Group Chief Information Officer, Standard Chartered, Singapore
- DATO' Dr. Haji Amirudin Bin Abdul Wahab - CEO, Cyber Security Malaysia
- Foo Siang-Tse, Sr. Managing Director, Quann Asia Pacific and many more

Market leaders partnered to make the event a one-stop shop for all security related challenges included Quann, Darktrace, Ixia, Apvera, Singapore Fintech Association, Singapore Computer Security, Cloudera, NTT Security and more.

Some of the topics of discussion included Malaysia's Initiatives in strengthening National Cyber Security, using Machine Learning for Next-generation Cyber Defense, Harnessing the benefits of Fintech with Application Programming Interfaces (APIs) and many such interesting topics.

The summit acted as a point of connection for CISOs and security professionals to be updated on the latest innovations in exponential financial technology and focus on how rising technologies can help solve security challenges; giving an opportunity to select the right kind of security vendors with the focus of having a global business vision and forging a win-win security situation. SST

Forcepoint Acquires RedOwl, Extends Global Human-Centric Security Leadership

Integration of RedOwl UEBA with Forcepoint technology delivers holistic view of cyber behaviors to identify and address enterprise risk in real-time

Singapore – Global cybersecurity leader Forcepoint today announced the acquisition of RedOwl, the leader in security analytics focused on helping customers understand and manage human risk. This latest milestone in Forcepoint's strategy arms customers with cybersecurity systems designed for the reality of today's threats.

Forcepoint's human point strategy views people rather than technology infrastructure as the focal point for

continue on page 30

cybersecurity. Cloud, mobility and ever-changing infrastructure makes the traditional perimeter a fallacy; by focusing on how, when, where and why people interact with critical data and IP, organisations can more effectively identify and address risk.

"The world has fundamentally changed and the way we think about security must change, as well. If the cybersecurity industry fails to put people at the center, it is certain to fall short in helping customers protect their most vital assets," said Matthew P. Moynahan, chief executive officer of Forcepoint. "Forcepoint is absolutely committed to empowering customers with human-centric security systems, and RedOwl fits squarely into this promise."

RedOwl's user and entity behavior analytics (UEBA) technology is ideally suited for this human-first approach to addressing security and regulatory use cases. Since 2011, the company has focused specifically on delivering capabilities that provide visibility into the holistic activities of people, including cyber, physical and financial. Customers deploy these capabilities to analyse large amounts of complex data, assess high-risk events and behaviors, and enact centralized and supervisory oversight to satisfy both security and regulatory requirements.

"As I've watched Forcepoint's story unfold, it is clear we share the view that a human-first approach must be the path to addressing cybersecurity and internal risk," said Guy Filippelli, chief executive officer at RedOwl. "The opportunity to deliver a holistic solution around

proactive human oversight is exciting; joining Forcepoint will accelerate our ability to deliver these important capabilities to our customers. We're thrilled to become a part of the Forcepoint team."

RedOwl brings a sophisticated analytics platform to Forcepoint's human-centric cybersecurity system and will be integrated across the company's portfolio, as well as with customers' existing technologies (e.g., SIEM). This platform delivers real-time insight into anomalous interactions and access across people, data, devices and applications. In addition, the combination of RedOwl's UEBA technology, Forcepoint DLP and Forcepoint Insider Threat will provide the industry's only comprehensive solution for understanding and responding to the behaviors and intent of people.

"Combining the deep collection capabilities of Forcepoint Insider Threat, the powerful analytics of RedOwl's technology and the risk mitigation of DLP creates a system capable of protecting critical business data and IP like no other," said Heath Thompson, senior vice president and general manager of the Data and Insider Threat Security business at Forcepoint. "Context is everything and we look forward to helping customers differentiate between carelessness, compromise and malice in the most efficient way possible."

RedOwl technology and employees are joining the Forcepoint team as part of the Data and Insider Threat Security business reporting to Thompson. SST

Kroll Names Paul Jackson Asia-Pacific Leader, Cyber Security and Investigations Practice, Hong Kong

Kroll Continues to Grow Cyber Security Practice Globally to Provide Clients with Time-Sensitive, Seamless Service

Hong Kong – Kroll, a global leader in risk mitigation, investigations, compliance, cyber resilience, security, and incident response solutions, today announced the appointment of Paul Jackson as Asia-Pacific Leader for its Cyber Security and Investigations Practice, based in Hong Kong. From a career spanning more than 25 years of service in some of the region's highest levels of law

continue on page 31

enforcement and corporate enterprise, Jackson brings a stellar record of achievement as a cyber security practitioner, strategist, and thought leader.

"I am excited to have Paul leading Kroll's Cyber Security practice in Asia. Not only does he possess deep knowledge regarding the region's diverse geopolitical and cultural complexities, he has developed a highly nuanced view of global cyber security challenges from working with organizations such as Interpol, the U.S. Secret Service's Electronic Task Force, and Microsoft's Digital Crimes Consortium," said Jason Smolanoff, Senior Managing Director and Global Cyber Security Practice Leader for Kroll. "This background combined with his experience leading large, high-performing teams dovetails perfectly with our goal of providing clients with the expertise and resources necessary to address their most complex cyber security needs, wherever they might arise in the world."

"Paul is a leader who possesses an invaluable perspective on the evolving cyber security threat landscape, from the most high-level strategic considerations to the most detailed operational components, all within a framework informed by regional and global realities," said David Fontaine, Chief Executive Officer of Kroll and its parent, Corporate Risk Holdings. "Having worked in law enforcement, a large corporate environment, and, most recently, as an external advisor to enterprises with global operations, Paul's experiences are well-suited to the needs of Kroll's clients in the APAC region and around the world. The addition of Paul to our team of Cyber professionals further reinforces our commitment to the global expansion of our Cyber Security practice."

Jackson started his career with the Hong Kong Police Force and over 22 years, rose through the ranks to become Chief Inspector and Head of the IT Forensics Practice, Investigation Team, and Training in the force's Technology Crime Division. In this role, he led multiple teams of cyber investigators, computer forensics examiners, and police college trainers, and was policy manager for digital evidence for the entire police force of 27,000 members. His accomplishments included overseeing the design and construction of a multimillion-dollar project to build the IT forensic laboratory and all associated IT security infrastructure; heading an internal "think tank" that provided top-level police management with strategic planning and policies relating to technology crime trends and IT security matters; leading the government incident response capability against cyber threats to critical infrastructure during major events such as the Olympics, WTO meeting, ITU Conference, and East Asian Games; and implementing an innovative incident response methodology for live (compromised) system analysis, which was ultimately adopted by Interpol and police forces worldwide. During his tenure, Jackson was also appointed by Interpol as course director for the Asia-Pacific Region to develop and deliver IT investigation and forensics training to law enforcement. His design and management of an advanced training facility for the HKPF was later used as a template by Interpol and the Korean Police University. Jackson brought to these training efforts a tremendous range of practical, frontline experience from his earlier roles as Head of the Computer Security Unit in the Crime Prevention Bureau, Head of the Telecommunications Liaison Office in the Criminal Intelligence Bureau, and a uniformed officer for eight years.

After leaving the HKPF in 2010, Jackson became APAC Head of Fraud and High Tech Investigations for JP Morgan Chase Bank, and from 2012-2014, he relocated to New York where he served as the bank's Global Head of High-Tech/ Cyber Investigations. In this role, Jackson managed a global team of cyber investigators and responders throughout the United States, Europe, and Asia, focused on addressing the pressing needs of managing the evolving threats faced by a global financial institution. Executing on these objectives involved among other efforts, redesigning global cyber laboratories and introducing new forensic technologies to enhance the efficiency and capacity of the team. In addition to serving as a strategy leader, Jackson personally conducted numerous investigations, successfully resolving several major incidents that included, among others, a well-publicised breach, data exposure, reputational issues, employee misconduct, insider threat, and electronic fraud.

Most recently, Jackson was APAC Managing Director

continue on page 32

for Stroz Friedberg. In this role, Jackson developed several of the firm's products and services with an APAC focus and personally led client engagements in cyber security assessments, C-level cyber incident table-top exercises, and data breach investigations. He also served as a thought leader and represented the firm in numerous venues, forums, and major public events.

Jackson earned advanced diplomas in Computer Forensics at the University of Science and Technology in Hong Kong, and a Bachelor of Engineering degree, with honors, in Engineering Science and Industrial Management at the University of Liverpool. In addition to holding a number of technical certifications, Jackson has been a Professor at the University of Defence, Science and Technology in Beijing since 2007, and a member of the China Computer Forensics Research Centre since 2008. He was also the only member selected from Hong Kong by the prestigious Network Security Professionals (NSP) Group, an organization of influential leaders from the world's largest network backbone providers; members are able to provide instant mitigation response to large-scale denial of service attacks. Jackson's other past and present affiliations include Asia Crisis and Security Group; the National Cyber-Forensics and Training Alliance, a leading U.S. group coordinating law enforcement and private sector collaboration against cyber crime; International Organisation on Computer Evidence; High Technology Crime Investigation Association; U.S. Secret Service Electronic Crimes Task Force; U.S. Financial Services Information Sharing & Analysis Center; and Microsoft's Digital Crimes Consortium. SST

Global Two-Way Radio Communications Provider Hytera Sues Motorola Solutions for Patent Infringement

Manufacturer of Professional Mobile Radio Solutions Files in U.S. District Court in Ohio, Claims Motorola Solutions Infringes Hytera's Patented Sound Adjustment Technology in Mobile Radio Handsets

Shenzhen, China - Hytera Communications Corporation Limited, the world's leading provider of innovative professional mobile radio (PMR) solutions, today filed a lawsuit against Chicago, Ill.-based Motorola Solutions, Inc. in federal district court in Cleveland, Ohio, charging that Motorola Solutions is infringing Hytera's U.S. Patent No. 9,183,846, which covers its industry-leading sound adjustment control technology.

Hytera's '846 patent is its inventive method for adjusting sound volume in response to background or ambient noise, allowing a radio operator to hear and speak over it. The device obtains the current level of ambient noise, receives an instruction, and adjusts sound output. If ambient noise is high, the volume adjustment is greater at higher (treble) frequencies. Hytera's complaint asserts that Motorola Solutions unlawfully misappropriates Hytera's patented technology for sound adjustment, incorporating it into its MOTOTRBO portable radios.

"Hytera has changed the landscape of the PMR business with its constant innovations, especially after its launch of a digital product line in 2010," said Tom Wineland, Director of Sales for Hytera Communications America (West), Inc. in Irvine, Calif. "Our patented sound adjustment functionality is one of the many innovations that Hytera has incorporated into our digital products, and users in markets around the world have embraced this feature."

Hytera's two-way radio communications equipment includes hand portables, mobiles, base stations, and dispatching and management software. Its products and solutions are used by commercial industries, such as energy companies and utilities, event organizers and producers, security and emergency management response teams, schools and other educational institutions, and public safety organizations. During use, personnel using Hytera's devices frequently move from quiet environments with little background noise to loud environments where machinery, engines, crowd noise,

continue on page 33

sirens, or other noises make it difficult to hear.

As embodied in the '846 patent, Hytera's sound adjustment capability is a key technological advance in PMR speaker design that is critical in a variety of noisy situations. "Our users—police and emergency responders, stadium and event managers, and commercial users—benefit greatly from this capability in our devices," adds Wineland.

"Motorola Solutions is infringing Hytera's sound adjustment control patent," said Andrew Yuan, Hytera's President of North and South America. "Hytera is a leader in innovative technologies, and an adamant advocate of intellectual property rights. We will look to enforce our patents in court in the U.S. and worldwide."

Hytera invests up to 15 percent of annual revenue in research and development, notes Yuan, including in open standard technologies, and is continually developing customized solutions that couple versatile LTE broadband for video and data transmission with traditional PMR narrow-band two-way voice communications. Hytera is one of the few companies worldwide that offers market-leading TETRA, DMR, and PDT technologies, and that offers products and solutions under all mainstream digital protocols. Hytera currently holds 480 issued patents, including 269 patents for digital products (DMR, TETRA, and PDT).

Hytera is the second-largest professional mobile radio communications solutions provider in the world, and the world's fastest-growing. Hytera also is the world's #1 DMR trunking provider. Hytera has partnered with companies in the U.S. since 2000, and established its first U.S. subsidiary, Hytera America, Inc., in 2004. Hytera established Hytera Communications America (West), Inc., in 2016 and opened research and equipment servicing facilities in the Chicago area this year.

Hytera further claims that Motorola has been and still is indirectly infringing Hytera's '846 Patent by actively inducing direct infringement by other persons who use products that embody one or more of the claims of the patent while Motorola had knowledge of the patent, knew or should have known that its actions would induce direct infringement by others, and intended that its actions would induce such direct infringement. Hytera is also alleging contributory infringement. Hytera is seeking damages and will pursue further relief as appropriate.

Hytera filed its lawsuit in the U.S. District Court for the Northern District of Ohio, in Cleveland, Ohio. The patent-at-issue is U.S. Patent No. 9,183,846 ("the '846 Patent") titled "Method and Device for Adaptively Adjusting Sound Effect." Hytera is represented in this action by Todd Tucker of Cleveland, Ohio-based law firm Calfee, Halter & Griswold LLP. SST

Miyoshi combines efforts with NEC Asia Pacific to market cutting-edge face recognition surveillance product in Asia Pacific

- *NEC's NeoFace® Watch Solution will incorporate Miyoshi's advanced situation response system ("SRS") and other core elements, and the new product will have wide application in homeland security, border control and law enforcements*
- *Miyoshi and NEC Asia Pacific will join forces in sales, marketing and publicity to maximize the sales of the product line*

Singapore – Miyoshi, an SGX-listed company and a regionally recognized Integrated Engineering Services ("IES") provider of advanced development and manufacturing solutions, announced today that its 100% owned subsidiary, Miyoshi Optoelectronics (S) Pte. Ltd., has entered into a joint marketing agreement with NEC Asia Pacific Pte. Ltd. ("NEC APAC"), for the two companies to jointly market

continue on page 34

a high-performance face-recognition surveillance related product in Singapore, Malaysia and other Asia Pacific regions.

The two companies are jointly launching a new line of products and solutions, which will consist of integrating NEC's NeoFace® Watch, a real-time facial recognition solution, into Miyoshi's wireless audio/video wearable solution trademarked as the Digital SRS, a highly reliable, low latency body-worn video/audio server/transmitter, COFDM1 streamer and COTS2 camera, with a personal ruggedised lithium battery on a Molle vest (the integrated solution is referred to as the "Product"). The combination of Miyoshi and NEC solution allows security officers on the ground instant analysis of what they see, enabling

them to provide actionable intelligence to commanders.

NEC's NeoFace®, an artificial intelligence ("AI") facial recognition engine boasting the world's highest authentication accuracy, generates real-time alerts when matching faces against a watchlist of individuals, thereby quickly finding a match for a person of interest.

Miyoshi and NEC APAC will work cooperatively to assess viable market segments, applications, and potential customers. They will also share market information, exchange customer leads, provide consultation to each other, and collaborate in publicity efforts. This powerful combination of two multinational companies' and their technologies already saw a pilot contract win in a Southeast Asian country's homeland security agency where the integrated solution is used daily for border protection and search and rescue missions in the northern borders. SST

Forcepoint Adds Seasoned Sales Leader for Asia-Pacific to Empower Customers with Human-Centric Security

George Chang joins as Vice President of Sales for APAC

Singapore – Global cybersecurity leader Forcepoint today announced it is further cementing Asia-Pacific operations to meet growing demand for human-centric cybersecurity solutions by appointing George Chang as vice president of sales. Chang is based in Forcepoint's Singapore office and reports to chief revenue officer, Sean Foster.

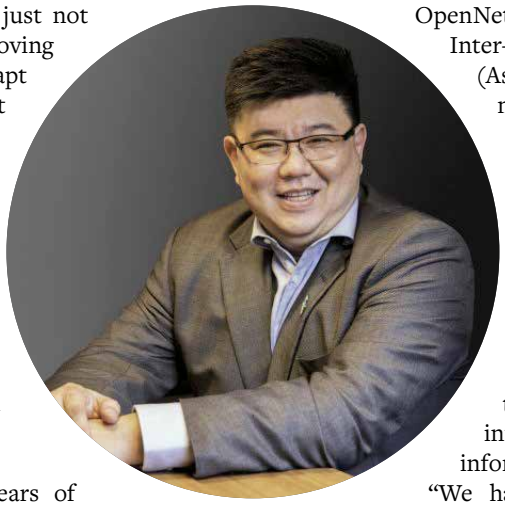
At Forcepoint APAC, Chang leads the company's growth strategy in the region and will drive customer engagement across the entire portfolio of Forcepoint's technology, including CASB, data loss prevention, insider threat, web security, email security and next-generation firewalls.

The appointment expands on the company's commitment to deliver insightful security solutions that help customers understand the rhythm of people in the organization and flow of critical business data and intellectual property – wherever it may reside. This people-first approach helps global enterprises and governments focus resources on activities that present the greatest risk to their business or mission.

"In the new digital and mobile world where there is no longer a perimeter, the detection and protection

continue on page 35

of data using point products is just not good enough. The market is moving to cyber solutions that adapt protection based on the context of user behavior, and we need inspirational and driven leaders to help customers and partners address this paradigm shift," said Foster. "George and his team will help lead the charge in delivering the most intelligent systems that facilitate business and foster productivity while stopping bad cyber activity."



Chang brings more than 20 years of experience in international business across the technology industry. Most recently, he served as regional vice president of APAC sales at Fortinet in Singapore. Prior to this, George held senior leadership roles in multiple technology companies including OpenNet Pte. Ltd., SYSTEX South Asia, Inter-touch Pte. Ltd., and STSN (Asia Pacific). George earned his master's degree in international business from the University of Technology in Sydney, Australia and a bachelor's degree in business computing from Queensland University of Technology, Australia.

"As the network perimeter dissolves, companies are looking to how, when and why people interact with data – and where this information travels," said Chang. "We have the unique opportunity to partner with Asia-Pacific companies to ensure their users and critical business data are protected everywhere. These organisations can maximise their investments by putting cyber behaviors at the center of their security equation." SST

"**Predictive policing, the process of using data and analytics** to anticipate where and when crimes will occur, has taken a lot of heat from critics who say it encourages discrimination against certain segments of the population and racial profiling. We can't say that's never happened. But we can offer the reminder that it is a disruptive technology, much like smart meters were several years ago. And like most disruptive technologies that have arrived in recent years, predictive policing is evolving and getting better. "

"**Many consider predictive policing** to be the future of law enforcement. It's in use in police departments in several states and cities from Santa Cruz, California to London report significant reductions in a variety of types of crime."

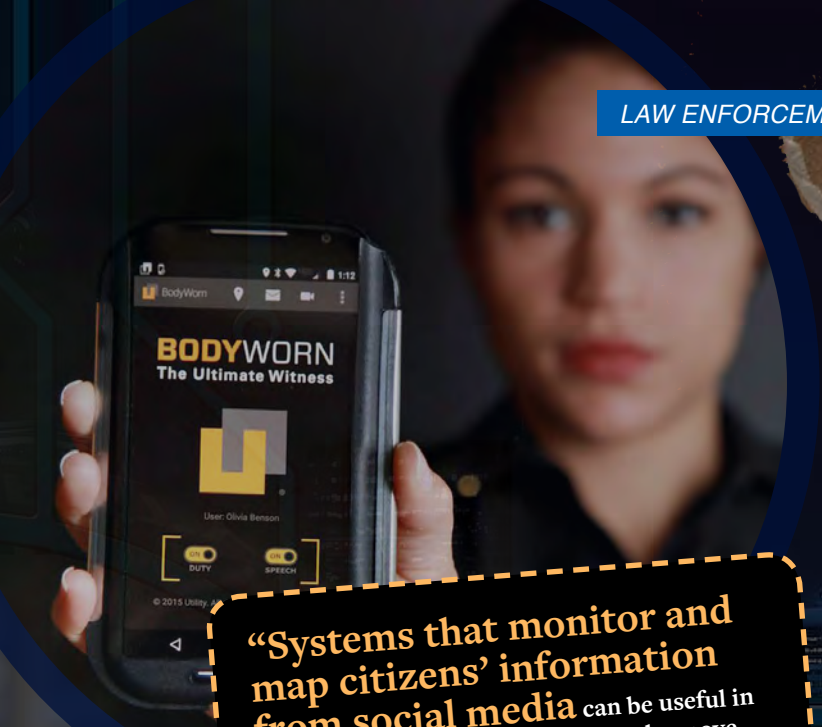
"**Be it sensors, microphones, cameras, radios or even drones, smart technology and big data analytics** are aiding emergency services in predicting and responding to critical situations. Looking forward, it is not so hard to imagine a smart city, filled with sensors, being able to take this concept further with eyes and ears on the ground providing crucial real-time information. In the continuous one-upmanship between criminals and law enforcement, the police are getting a little bit smarter."

LAW ENFORCEMENT

Crime Fighting Goes Digital

"**Council Lead Partner Microsoft also has been heavily involved.** Its Azure Government end-to-end cloud solution was chosen by predictive policing solutions company PredPol, a company popular with law enforcement agencies. PredPol's system uses an algorithm to predict where and when crimes will probably occur based on criminal behavior patterns and provides maps to police to help them zero in on areas where there is a good likelihood that they can prevent crime."

"**Technology giant Cisco is getting in on the smart emergency response sector** with its IPICS emergency response interoperability system. In emergency situations such as earthquakes and fires, Cisco IPICS allows rapid response from emergency teams as well as providing information other relevant groups, such as human resources or corporate crisis management teams. Using an end-to-end radio dispatching solution Cisco's Dispatch Console client is the link between dispatchers and field personnel, helping coordinate a smart response and increasing safety in cities in times of crisis."



GETS SMART

"Systems that monitor and map citizens' information from social media can be useful in situations where the suspect is on the move, in a sense gathering witness statements from several people across a wide geographic area. Alternatively, citizens can also be alerted quickly with programs that push out important information to mobile devices of people in a particular area."

"Sensor programs like PredPol or Palantir can be used to identify patterns and even predict when and where crimes are most likely to occur. These tools can register and report early indicators of an emergency or crime, or help department gather information about underreported crimes.

"Safe Cities is all about taking disparate technologies, integrating them using IoT connectedness, and using the resulting system to make citizens more secure in the public environment."

"If actually accurate, predictive policing can fundamentally change the way law enforcement reacts, or proacts, to illegal and dangerous activities, making our smart cities safer. That is until SMART criminals start using this data to avoid SMART police."

"ShotSpotter, as mentioned above, is just one kind of environmental sensor. Other sensor programs like PredPol or Palantir can be used to identify patterns and even predict when and where crimes are most likely to occur.4 These tools can register and report early indicators of an emergency or crime, or help department gather information about underreported crimes."

"Predpol , the predictive policing company is providing law enforcement agencies with customized crime predictions for the places and times that crimes are most likely to occur. Using just three data points – past type, place and time of crime – PredPol created a unique algorithm to analyse criminal behavior patterns, which they say can then be used to accurately predict the time and location future criminal activities."

Smart Cities -Safe Cities: Intelligent Cities

Genetec Inc. Director of Strategic Markets, Pervez Siddiqui, discusses the needs and challenges for assuring that cities are not only 'smart,' but also 'safe'—a crucial, core component of any metropolitan area as it evolves over time.

According to the World Health Organisation (WHO), one hundred years ago, two out of every ten people lived in an urban area. Today, more than half of all people live in a metropolis, and by 2050 these figures are set to increase by 70%. This pace of urbanisation calls for cities to make smarter decisions about how they allocate their resources. With these great migrations to urban areas come many new challenges, including assurance that all city dwellers can live harmoniously in a 'safe' city, served by 'Smart City' technological advances. Yet, the reality in most cities is that the two conversations—those relating to the safe city and the smart city—are distinct and siloed.

Over the past four years, a growing number of mayors and CIOs have promoted the idea of building a Smart City as part of a broader strategy, to attract and retain residents, talent and businesses. After all, most cities are in competition with other cities and need to differentiate themselves just like private organisations do. There is a near-weekly drumbeat of announcements indicating yet another program planning to pilot a Smart City concept.

About the Author

Pervez Siddiqui is the Director of Strategic Markets at Genetec Inc. He is a firm believer in the need to bring together urbanists, security experts, public officers and private enterprises to examine how cities operate and can be improved to create more vibrant, exciting and safe spaces that attract and retain residents, companies and communities.

"The concept of the Smart City is founded on a utopian vision. In steady-state, sensors embedded in virtually every aspect of our urban infrastructure, will collect data, communicate with each other and make sense of the data. The most advanced implementations will be those which will also detect unnatural patterns in the data, represent the data in a meaningful manner and even make smart decisions in response to this data."

The concept of the Smart City is founded on a utopian vision. In steady-state, sensors embedded in virtually every aspect of our urban infrastructure, will collect data, communicate with each other and make sense of the data. The most advanced implementations will be those which will also detect unnatural patterns in the data, represent the data in a meaningful manner and even make smart decisions in response to this data. Oft-cited examples of the Smart City in practice include self-driving vehicles which communicate with other vehicles, and infrastructure to ensure smoother traffic and fewer accidents. Another example, which is particularly salient given the LED advancements underway around the world, is that upgraded street lights can also capture security and traffic intelligence to help feed other functions to make the city safer.

A specific concern however, as cities expand to add layers of information-gathering systems and software to support their 'smart city', is that vulnerabilities will also increase. This is where Genetec as a technology innovator is playing an important role to assure that the incredibly high volume of data for the city is not only secured and 'hardened' against cyberattacks, but is also encrypted for privacy .

Many cities work with disparate, proprietary 'brittle' data systems that were designed to meet specialised needs, but today, are no longer relevant or usable as needs have evolved. These customised systems cannot be sustained, and in many cases, due to budgets, lack of ownership, limited IT support or compatibility complications, require complete (expensive) overhauls. By adopting an open-architecture system that can scale to accommodate growing data, and mitigate software risks with the latest 'Security of Security' measures—smart cities will have the information infrastructure necessary to grow and assure their cities have the best analytic data, protected from cyberattack with privacy protections for the public.

Despite the ambiguity or challenges of data from different stakeholders, there is a general consensus that a Smart City is one through which technology is made (a) decidedly less frustrating, (b) more vibrant, (c) more transparent and accountable, and/or (d) more efficient. The other reality is that the use of sensors and connected devices within cities is growing and will continue to do so into the foreseeable future.

While there may be a range of perspectives on what the Smart City is, the "safe city" concept is far less abstract. More often than not, most associate the safe city concept with surveillance used by the police force to fight crime. However, in reality it must be extended much more widely to incorporate the likes of economic safety (safety of the infrastructure which ensures the community's livelihoods), and civil safety—such as those which relate to the integrity and safety of bridges, pedestrian lanes, bike lanes, and intersections.

Viewed at a high level, the aims and ambitions of realising a city that is both smart and secure do not conflict. Urban design and an infrastructure of technology can and should reinforce one another to deliver solutions that work on different levels. However, initiatives do have to take account of the reality that a living, breathing city will always be made up of multiple stakeholders – public and private – each with their own key concerns and priorities. It is here that initiatives can fall down as a lack of joined-up thinking

"Forming the right partnerships and answering the above questions takes time but it really is a prerequisite to building a smart, safe and above all, intelligent city that works. Technology can take us only so far, but by bringing together the right people, and forming the right partnerships, we can build a model flexible enough to adapt and evolve that proactively meets the ever-changing needs for urban inhabitants."

can doom even the most technologically-equipped implementation to failure.

For instance, in many cities the large sporting stadiums are private enterprises whose activities will have major impacts on other stakeholders within the metropolitan area: police, local government and the transit authority to name just a few. Inevitably, the primary concern of law enforcement will be to ensure the security and safety of everybody attending the game. Meanwhile the transport authorities will be just as concerned about controlling the flow of traffic around the stadium to ensure any impact to other aspects of the city such as access to the shopping district or to hospitals in the area is maintained. Finding a happy balance involves a little bit of give and take on both sides; the stadium can never be allowed to become a 'soft target' or a citizen-unfriendly 'ring of steel' in pursuit of one of these requirements. Plus there is no practical reason why the same underlying infrastructure can't be deployed to the mutual benefit of both parties. For example, existing traffic cameras in the area could continue to be monitored on an on-going basis with a separate feed piped to a law enforcement control room only on match days. If this gave police better visibility of approaches to the stadium and prevented the need to set up road blocks that slow down traffic flow it really would be a win-win for all concerned.

From a technological standpoint, this is very simple and cost-effective. However, it can only come to fruition if stakeholders within the city who don't usually find cause to speak to each other choose to come together and actively collaborate.

This takes a great deal of effort but does not need to be expensive, as it does not require every individual stakeholder to share one giant system. The cost of procuring, configuring and maintaining a single system that could meet the individual needs of each party would be prohibitive to say the least. Instead we advocate a concept that we call Federation which sees each player maintain access to their own open platform system, simply with the option to share access with others in municipality when there is a compelling reason for them to do so.

This will, of course, prompt multiple questions for each individual stakeholder within the larger Smart City initiative: How do we balance the need for trust versus the need for agility? How do we exercise control of our data when we start sharing across enterprise boundaries? How do we ensure the veracity of the data and chain of custody? How much do we share? When do we share and do we only share certain data in very specific public safety circumstances such as in the immediate aftermath of a significant critical incident?

Forming the right partnerships and answering the above questions takes time but it really is a prerequisite to building a smart, safe and above all, intelligent city that works. Technology can take us only so far, but by bringing together the right people, and forming the right partnerships, we can build a model flexible enough to adapt and evolve that proactively meets the ever-changing needs for urban inhabitants. SST

Body Worn Cameras Now Crucial for First Responders

Edesix to demo full range of body worn cameras utilised by emergency services around the globe

Edesix, market leaders in the provision of body worn cameras, showcased how its fleet of body worn cameras are becoming increasingly important to the safety and development of first responders around the globe at the 2017 Emergency Services Show.

At the show, Edesix demonstrated its newly launched VideoTag (VT-50), its smallest incident recorder to date, as well as the VideoBadges utilised by Police Services Northern Ireland, South Australian Police, Her Majesty's Prison Services and West Midlands Fire Services.

VideoTag

Edesix's VideoTag is its smallest, lightest and most discreet incident recorder to date and is proven to deter aggression, protect staff and provide secure evidential-quality footage on demand.

Designed for less frequent use than Edesix's VideoBadge body worn cameras, the VideoTag is lightweight, unobtrusive, cost-effective and easy to use. It requires no extra training, streams live footage, and has a standby battery-life of up to three months meaning users don't need to worry about charging the device often. The VideoTag also provides complementary audio and video capture of incidents when utilised as part of a larger body worn camera and CCTV security function.

Police

Police on the front line have found that body worn video helps prevent both criminal and anti-social behaviour when out on patrol. Additionally, the captured footage not only provides greater transparency of the interactions with the public, but can also significantly increase early guilty pleas when used in a prosecution.

Edesix's VideoBadges are currently utilised by Police Forces around the globe, including Police Services Northern Ireland, Police Scotland and South Australian Police. Superintendent David Moore, from PSNI, where over 400 VideoBadges have now been deployed, commented: "Video evidence puts the victims of crime first. The pilot of this technology in Foyle district evidenced how Body Worn Video has the potential to improve the quality of evidence provided by Police officers and thereby increase the number of offenders brought to justice."

Prisons

Edesix is the preferred supplier for the UK Prison Service nationally. However, it is the sophisticated solution provided by the company, inclusive of bespoke hardware and software, which benefits the service most.

The hardware and infrastructure provided by Edesix ensures efficient workflow and ease of use for prison officers, and those managing the data. Using a combination of DockControllers (a device which allows up to 84 VideoBadges to be connected, assigned and managed from one instance of VideoManager) and MicroServers

for data storage; large estates of cameras can be simply rolled-out and centrally managed.

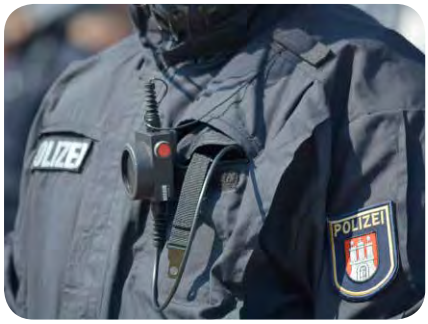
Although complex in its design, the Edesix solution ensures that the day to day operation of prison-wide BWCs is simple to manage, unobtrusive for staff, and easily scaled upon demand. The cameras worn by prison officers are capable of recording up to eight hours of footage including audio, and come with flexible mounting options for uniforms. The entire solution is secure and encrypted, meaning that even in the worst circumstance, a lost or stolen camera's footage cannot be viewed, deleted or shared.

Fire

In 2016 Edesix became one of the first BWC providers to supply fire services in the UK. After a successful trial at ten Birmingham fire stations

continue on page 43

in 2016, Edesix currently supplies fire-fighters in the West Midlands with its VB-300 series of Body Worn Cameras - its first generation of WiFi enabled VideoBadges.



West Midlands Fire Services are also conducting trials on Edesix's X-100 side-mountable tactical head cameras, which are connected to the VB-300. The X-100 offers automatic rotation of footage, meaning it can be worn on either side of the head without requiring user configuration to rotate footage. It is connected to a VB-300 with a convenient two-part cable for easy removal, which allows a VB-300 to be situated under a uniform or on a belt pocket.

Watch Commanders attending call outs throughout the West Midlands are now equipped with VideoBadges to help share best practice techniques and complement firefighter training, ultimately improving the service's operations well into the future.

For more information,please visit www.edesix.com SST

Consortium Fields a Successful Smart City Pilot Project in Singapore

Across the world, cities are evolving at a rapid pace with many changes being made in favor of infrastructure that can help cities efficiently manage events and resources across multiple agencies. Singapore is an example of one such city.

As a pioneer in the development of smart city infrastructure and with these challenges top of mind, AGT International is constantly on the lookout for ways to innovate and harness the power of the Internet of Things (IoT) and relevant public data to develop groundbreaking solutions that meet the basic needs of citizens and allow intelligent decision making.

Working directly with the Singapore government, we initiated the Singapore Safe SmartCity test bed pilot project as part of a consortium with O'Connor, and Hitachi Asia, a regional subsidiary of Hitachi, Ltd. Through the pilot we created an integrated multi-agency solution that could easily be implemented within the existing city infrastructure and offer greater insight into its daily operations, a key function needed to make the city smarter. The platform we used is called CityMIND and is powered by AGT.

The CityMIND platform uses our advanced analytics in addition to web intelligence, powerful sensors and big data to connect various interfaces and outputs, from video and facial recognition cameras to smart phones, in order to create a comprehensive and reliable view of the city. Today, we are especially pleased to announce the success of this initial pilot, which trialed the recently launched CityMIND 6.5 platform. We are certain that it will serve as a model that other major cities can follow, underscoring the importance of IoT based technology in improving smart city development.

The key to ensuring our success in Singapore was to take a city that was already very forward-thinking and introduce a platform that helped to facilitate knowledge sharing among constituents and better real-time communications between government agencies and all

continue on page 44

parts of the city to get every urban stakeholder – both public and private – working together in support of a common goal. Through CityMIND, a number of key smart cities technologies were implemented successfully in Singapore, to identify traffic congestion and crowding, improve cleanliness by using sensors in trash bins to automatically signal when they need to be emptied, increase communications between first responders, authorities and citizens with specially-designed mobile device applications and raise awareness of relevant social media trends.

Research shows us that early adopters in smart city implementations like Singapore will be the cities that thrive over the next 10, 20 or 50 years, while cities that do not will ultimately become less competitive. Our experience tells us that cities are exactly where leveraging IoT can enable the most dramatic improvements of all for citizens so we are very excited to be at the forefront of technology that is developing smart city initiatives.

We also feel honored to have been given the opportunity to support Singapore, which is already much more developed than other cities in many ways, and help the government to address larger, forward-looking issues. Given its success, we believe that the pilot project in Singapore can be leveraged as a use case that governments in cities across the world facing similar growth and infrastructure management challenges can look to.

> *"The CityMIND platform uses our advanced analytics in addition to web intelligence, powerful sensors and big data to connect various interfaces and outputs, from video and facial recognition cameras to smart phones, in order to create a comprehensive and reliable view of the city."*

Our goal in participating in the consortium and working through the pilot is to help governments easily assess the positive role that safe-smart integration can play in protecting citizens and drive that agenda globally.

For more information, please visit: www.agtinternational.com SST

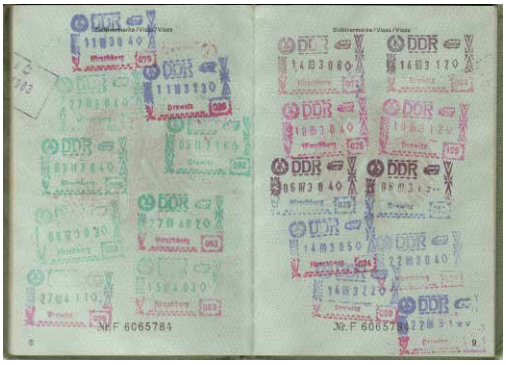
Gemalto Enables Biometric Passports in Over 30 Different Countries

Singapore - Gemalto, the world leader in digital security, announces that its advanced epassport technologies are now being used in over 30 different countries. Thanks to their outstanding security and the faster, more convenient border crossings they facilitate, the company's solutions help authorities strengthen homeland protection and improve the traveller experience. Gemalto's leading

continue on page 45

position has been built on the supply of complete travel documents and key components such as polycarbonate data pages, visible and hidden document security features, electronic passport covers and ICAO-compliant embedded software. In addition, the company's secure embedded software has consistently outperformed the competition in international tests on speed over the last decade. Gemalto is also making an active contribution to the definition of international ePassport standards.

Introduced in 2005, the ePassport – which now represents 57% of passports in circulation - delivers enhanced fraud protection by incorporating a secure microprocessor that stores the holder's personal data and digital photo. Electronic passports include a standardised electronic portrait of the holder for facial recognition, which opens the door to a comprehensive range of automated, self-service airport services for passengers. This extends from check-in through to immigration control and boarding, resulting in an enhanced experience on arrival and departure.



The Future ePassport

A new generation of ePassport will digitally store travel information such as eVisas and entry/exit stamps to support even more efficient immigration control. The key trends in travel documentation identified by Gemalto include:

Swift migration to tamper-proof polycarbonate data pages, which dramatically reduce the risk of fraud.

Rapid growth in secure digital identity credentials. Sensitive ePassport data is stored on the holder's smartphone to create a secure companion to the physical passport, making life easier for travelers.

Smart borders/smart airports to emerge at a faster pace. Combined with the hundreds of millions of ePassports now in circulation and a strong push behind biometrics (particularly facial recognition), they offer travelers quick and secure cross-border movement.

"Over the past decade, Gemalto has helped develop some of the world's most secure and attractive ePassports, including landmark projects in Algeria, Denmark, Finland, France, Hong Kong, Italy, Korea, Morocco, Peru, Portugal, Norway, Singapore, Sweden and the USA." said Youzek Kurp SVP ID Document Solutions, Government Business Unit, for Gemalto. "Our success is based on close collaboration with partners, ensuring that the unique requirements of each project are always fully realised." SST

Honeywell Helps Bhubaneshwar Boost Security with City-Wide Surveillance System

Honeywell technologies a key enabler in making Bhubaneshwar a SMART city

Honeywell announced that it is helping Odisha Police with a city-wide surveillance system that helps boost security, prevent crimes, maintain law and order, and control traffic in the state's capital city. The quality of the city's security is exemplified by Bhubaneshwar's recent win at the World Smart City Awards. The recognition from the Smart City Expo World Congress is a testimony of Bhubaneshwar's transformation by adopting cutting-edge technology for resolving urban challenges

The Honeywell project provides 28 strategic locations in the city with 114 integrated closed-circuit televisions and automatic number plate reading cameras using a command and control system that provides a common operating picture, interactive control, event correlation, and mobile van surveillance in the Police Commissionerate headquarters.

continue on page 46

"We are happy to work with Odisha Police to support their progressive approach to smart safety in the city. At Honeywell, our continued focus is on making cities smarter, safer, and more secure, in support of India's 100 Smart Cities vision. We are proud that our expertise is helping our partners and are delighted that Bhubaneshwar has been recognised by Smart City Expo World Congress for its tremendous efforts," said Aseem Joshi, regional general manager of Honeywell Building Solutions in India.

For better situational awareness, mobile cameras and digital video recorders have been installed on 33 police vans. These cameras transmit recordings at a pre-determined frequency to the command centres. The cameras are designed to withstand high day-time temperatures. Red-light violation detection systems and advanced video analytics help alert police about traffic violations and enable prompt incident management.

Honeywell is uniquely positioned with the broadest technology solutions portfolio to support India's 100 Smart Cities vision. It is already working on projects in Aurangabad in Maharashtra, an 11-city project in Madhya Pradesh, including a successful Ujjain Simhastha Kumbh event.

For more information, please visit: www.buildingsolutions.honeywell.com SST

Milestone Video Software Gives Italian City Visual Advantages in Attracting Tourists

Challenge

San Lucido in Italy is dependent on tourism, and needed a way to keep the city safe and attractive for citizens and tourists. The first step was to use technology to heighten the security level in the city to deal with incidents, improve city cleanliness and avoid graffiti in public areas. San Lucido also wanted to become more environmentally friendly by finding a way to keep the city clean and tidy for the benefit of the tourists and for the convenience of the citizens.

They needed a solution that could grow with the city and help them utilise technology to become a Smart City –a city using a digital infrastructure to perform better services.

Solution

Milestone Partner GSA di Guido Luigi based in Polistena RC, installed Milestone X Protect Express to manage 36 Axis cameras located in public areas in the city such as streets, parks and public buildings.

The local policeand security managers of public institutions can get an overview of all cameras with Xprotect Smart Client, an easy to manage timeline that enables the police to examine incidents quickly and make informed decisions.

The Milestone Mobile client for smartphones enables rapid response by the local police force as they can have full situational awareness even when patrolling.

continue on page 47

Advantage

San Lucido has successfully entered the first phase of becoming a Smart City. Because of the high image quality,surveillance video can be used to identify perpetrators or graffiti painters.

Abandoned waste can easily be detected to ensure the city stays an attractive tourist destination. Because of Milestone's open platform technology San Lucido can integrate with third party software to become even smarter in the future. The city is also able to expand the solution easily to cover more parts of the city.

Milestone helps San Lucido to be an attractive city to tourists and citizens San Lucido is heavily dependent on tourism as a source of income for the local businesses. A high level of safety is a very important factor forbeing an attractive city to tourists and local citizens.

Another factor is the cleanliness of the city. Waste in the streets is a burden to the environment if it is not detected and disposed correctly and rapidly.The city also has to cover the cost of cleaning up and disposing the garbage left in the streets. With the Milestone video security system they are able to give the wrong doers a fine in case of illegal dumping and make sure to remove the waste to ensure a clean city for the benefit of inhabitants and tourists.

The city's plan to become a Smart City is a part of a larger project initiated by the European Union with the goal of improving the quality of life and making cities more sustainable. The Smart City concept overall includes making better use of resources and ensure less pollution. It means smarter urban transport, upgraded water supply and waste disposal, and more efficient ways to light and heat buildings.

It also encompasses a more interactive and responsive city administration and safer public spaces. San Lucido has entered the first phase of their Smart City initiative. In this phase they want to heighten the security level at all public areas to ensure a safe city for inhabitants and tourists. The focus is primarily on avoiding misdoings, graffiti and other destruction of public property.

The city also wanted to become more environmentally friendly by finding a way to deal with garbage dumping in the streets. Milestone Mobile improves service quality Milestone Partner GSA di Guido Luigi based in Polistena RC, installed Milestone XProtect Express to manage a mix of motorised speed dome cameras and fixed cameras from Axis. The 36 cameras are located in public areas in the city such as streets, parks and public buildings.

The city police and security managers of the different public institutions have access to the video security system to ensure that the relevant authorities have situational awareness of the city.

San Lucido also uses Milestone Mobile allowing police and security managers to remotely monitor the public areas. That enables them to check up on different locations even when they are not near a computer. A police officer out patrolling in one area of the city will be able to check up on other parts through a smartphone enabling the local police to always be on top of the situation.Officers will be alerted if an alarm goes off by the alarm manager in XProtect Smart Client or by getting a push notification in the Milestone Mobile app.

The images received by the officers will be real time, giving them the possibility for rapid and more efficient response. San Lucido city has recognised the value in investing in the future city and is already talking about rolling out next phase of the project: "We have taken the first steps to become a city of the future with the help of Milestone's video software. We are also considering integrating Milestone's software with other technologies such as license plate recognition and video analytics to become a true Smart City," says Fabio Frangella, Security Councilor, San Lucido City.

Easy to Expand the Solution

Milestone XProtect is built on an open platform technology so San Lucido can easily add other

> *"We have taken the first steps to become a city of the future with the help of Milestone's video software. We are also considering integrating Milestone's software with other technologies such as license plate recognition and video analytics to become a true Smart City"*
>
> ***- Roberto Pizzutti, Mayor, San Lucido City***

continue on page 48

> *"San Lucido also uses Milestone Mobile allowing police and security managers to remotely monitor the public areas. That enables them to check up on different locations even when they are not near a computer. A police officer out patrolling in one area of the city will be able to check up on other parts through a smartphone enabling the local police to always be on top of the situation.Officers will be alerted if an alarm goes off by the alarm manager in XProtect Smart Client or by getting a push notification in the Milestone Mobile app."*

technologies to reach their goal of becoming a Smart City. Besides LPR software and video analytics the city is also thinking about integrating Milestone XProtect with traffic classification software to clear traffic jams. They are also considering doing an integration that connects an audio IP speakers system with the tourist information panels located at the different sightsto improve the experience of visiting the city for tourists.

Because of the open platform technology everything is made possible. A smart city uses digital technologies or information and communication technologies (ICT) to enhance quality and performance of urban services, to reduce costs and resource consumption and to engage more effectively and actively with its citizens.The flexibility and future proof design of Milestone's video software enables cities to reach these goals and become metropolitans of the future.

For more information, please visit:
www.milestonesys.com SST

Morse Watchmans Key Control System Streamlines Efficiency at Bustling Municipal Work Depot

Automated Tracking, Centralised Control Add to Depot's Operational Effectiveness in Major Suburban Community outside Sydney, Australia

Blacktown City is a bustling suburban community located approximately 22 miles west of Sydney, in New South Wales, Australia. Comprising 48 separate communities with a total population of 350,000, the city is the second largest city by population in NSW. The area is governed by Blacktown City Council which is responsible for all aspects of the city's day-to- day operation, project development initiatives and legislative activities.

Along with the City Council headquarters in the Civic Center, Council facilities also include the Main Works Depot located in the Blacktown City community of Rooty Hill. Council vehicles, heavy machinery and trucks as well as an operational work site for crews and other Depot employees are housed at this location. The Depot supports the operation of numerous city venues and development of zoned and serviced industrial and commercial land.

continue on page 49

To help maintain usage accountability and eliminate the problem of missing or overdue vehicles, machinery and/or building keys, the Depot recently implemented a key control and asset management system from Morse Watchmans. The new KeyWatcher® Touch is designed to securely store physical keys in tamper proof cabinets, only allowing access to keys by authorised individuals with a verified code, badge, or biometric identification.

Access to the key cabinet and to individual keys is under the complete control of Depot management and the automatic tracking provides full accountability for who has which key at any time.

"We manage keys for at least 500 vehicles and machines here at the Depot and each of them has at least two to three sets of keys," said Joe Haddad, Facility Manager, Main Works Depot. "Without the KeyWatcher Touch automated control and tracking, the job of accurately keeping track of these many keys would be almost impossible."

An important aspect of managing the large Depot is employee productivity and the design of the KeyWatcher Touch conforms to this by making the process of accessing or returning keys faster and easier for employees. Keys can be returned to any of the several key cabinets on site rather than having to return the key to the cabinet from which it was removed. Biometric identi cation, large, easy to read touch screens, voice cues, and status bar guides help to ensure a fast and easy procedure when accessing or returning keys to the cabinet. Key reservations ensure that sta will have guaranteed access to a vehicle or machine when needed.

The system automatically tracks the location of each key stored in a key cabinet or, if the key has been removed, the system can determine who has it out. Access to live information via the desktop or mobile lets department managers see which keys are out, if any keys are overdue, and when keys will become overdue. And for immediate information regarding a key, special alert notifications using email or SMS text provides the data instantly.

> *"The new KeyWatcher® Touch is designed to securely store physical keys in tamper proof cabinets, only allowing access to keys by authorised individuals with a verified code, badge, or biometric identification. "*
> *"The single platform for control of our video surveillance, access, and key management streamlines the operation, keeps costs down, and helps to ensure that nothing falls through the crack."*
>
> ***- Joe Haddad, Facility Manager, Main Works Depot***

Network integration of the KeyWatcher Touch with the Depot's access control and video surveillance system further adds to its ease of use and productivity. User access programming including add/modify/delete cardholders and badge data is managed through Inner Range's Integriti access control system and all changes are automatically synchronized. Alarms and transactions are passed to the Integriti system via the Depot's TCP/IP connection.

"The single platform for control of our video surveillance, access and key management streamlines the operation, keeps costs down and helps to ensure that nothing falls through the cracks," adds Mr. Haddad. "We are very pleased with this state of the art system and it has more than met our needs both today and, we expect, going forward.

The system was designed and built by system integrator Australian Security Technology (AST), a leading provider of key and asset management solutions in the Pacific region. Working with AST, Ryalex Security, a commercial security specialists company, helped bring the project together for Blacktown City Council.

"Blacktown City Council is a long-time customer and it was important that we help them solve their key control problems as efficiently and cost effectively as possible," said David Ishak, General Manager, AST. "The KeyWatcher Touch provided the solution to the great satisfaction of both the Depot and ourselves."

For more information, please visit:
www.morsewatchmans.com SST

Strategic National Projects to Build Singapore As a Smart Nation

The Smart Nation initiative is about harnessing the full power and potential of digital and smart technologies to create new jobs and business opportunities, in order to make our lives more convenient, and our economy more productive, through more efficient Government and business processes. But beyond that, a Smart Nation is about creating new opportunities in a digital age, and transforming the way people live, work and play, so that Singapore remains an outstanding global city.

Why the Push for a Smart Nation?

At the fundamental level, Smart Nation is about making daily transactions easy and seamless, be it making a payment, applying for a permit, etc. The technology that enables this smooth process should be invisible, and the design should be intuitive, so that the solution is not just convenient, but a delight to use. At a broader level, Smart Nation is about achieving efficiencies and effectiveness, be it leveraging sensors and data to better manage traffic or monitor security threats. Cost savings brought about by digitisation is also key to growing businesses. Citizens can use technology to improve quality of life, be it through monitoring health, reducing time spent on administrative tasks, or planning commutes, etc. But most importantly, Smart Nation is about transforming Singapore's economy, and ensuring that there will be jobs and opportunities in the future.

As an open economy, Singapore is impacted by global forces – geopolitical tensions, potential threat of anti-globalisation, and technology disruptions across many industries. Internally, there are challenges such as an aging population. Singapore however has strengths and achievements that place the country in a good position to succeed in Smart Nation.

As part of the Smart Nation journey, the Government has also been actively using digital technology to better serve the public. For example, the recently announced Singapore Student Learning Space (SLS) for various primary and secondary schools is an initiative that empowers students towards self-directed learning and soon, motorists will be able to pay for parking charges at public car parks via a mobile app, in place of paper coupons.

Strategic National Projects

However, there is a real danger that Singapore could fall behind in emerging areas, such as e-payments and digital identity systems. Singapore needs to do more, and with a renewed sense of urgency. The Government is therefore taking a more integrated approach to lay the foundation infrastructure, and drive pervasive adoption of digital and smart technologies throughout the economy and society. In the immediate months, the Government will focus on the following strategic national projects:

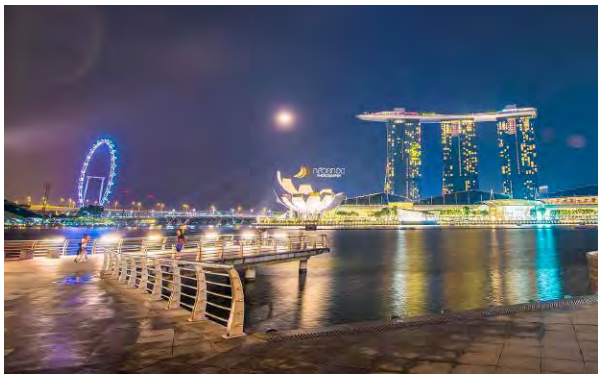
- National Digital Identity framework, for citizens and businesses to transact digitally in a convenient and secure manner;
- e-Payments drive, to allow everyone to make simple, swift, seamless, and safe payments;
- Smart Nation Sensor Platform, to accelerate the deployment of sensors and other IOT (Internet of Things) devices that will make our city more liveable and secure;
- Smart Urban Mobility, to leverage data and digital

continue on page 51

"At the fundamental level, Smart Nation is about making daily transactions easy and seamless, be it making a payment, applying for a permit, etc. The technology that enables this smooth process should be invisible, and the design should be intuitive, so that the solution is not just convenient, but a delight to use. At a broader level, Smart Nation is about achieving efficiencies and effectiveness, be it leveraging sensors and data to better manage traffic or monitor security threats."

technologies, including artificial intelligence and autonomous vehicles, to further enhance the public transport commute;

- Moments of Life, which bundles relevant government services, across different agencies, to the citizen at key moments of his life. This reduces the need for citizens to transact with multiple government agencies, for a more seamless and convenient experience.



To achieve the above outcomes, the Government will actively engage citizens and businesses, respond to their feedback and needs, and create space for innovation and co-creation. The Government is also in the process of crystallising the next phase of similarly impactful projects to advance Smart Nation, and will seek views and perspectives from different sources. SST

Raytec IP Lighting Combats Crime at Historic Manor House

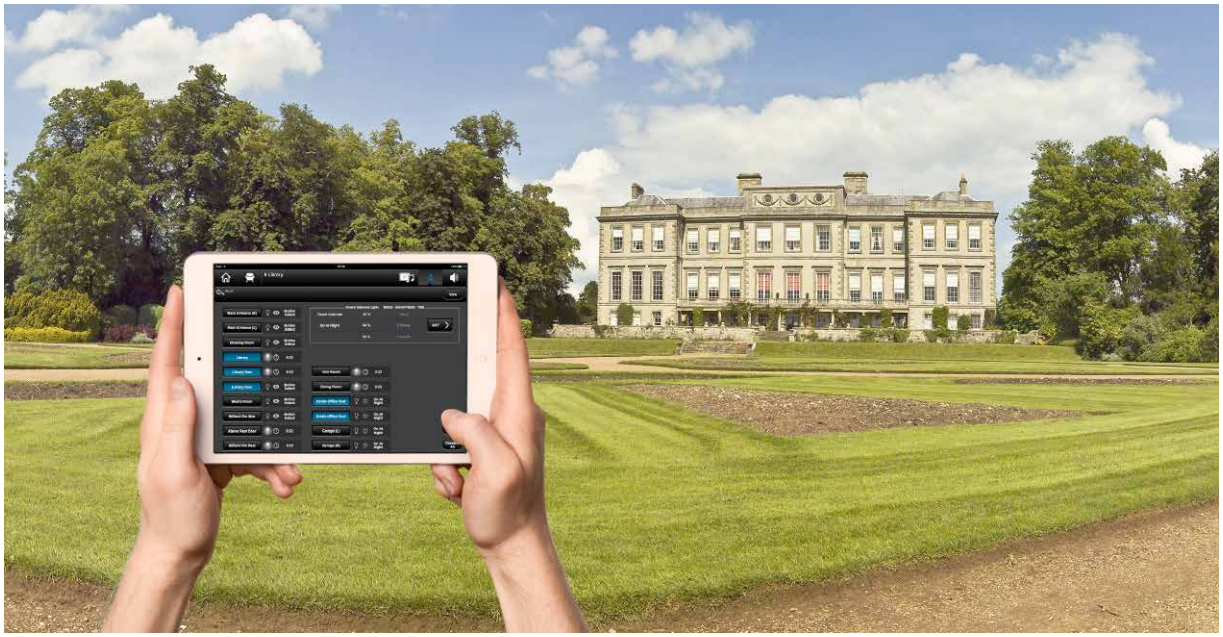
Raytec Network Illuminators have been deployed as a key element of a bespoke IP security solution for a Grade II listed Manor House in Shropshire, UK to deliver outstanding night-time surveillance images and actively combat crime.

Previously a target of crime, the estate had no professional CCTV system, relying only on halogen lighting with inbuilt PIR detectors. The security team needed a solution which would allow 24/7 monitoring over the property, particularly at night, with the ability to respond instantly to any security breaches.

SMC, leaders in electronic system design and installation, were responsible for designing the solution. They designed a state of the art IP surveillance system, fully integrated with Raytec White-Light IP Illuminators which were installed around the estate perimeter and around the Manor House. IP addressability and connectivity was crucial to the system design, ensuring that the IP lighting could be automatically triggered by any network device to provide an instant, visual response to any incident in real-time.

A bespoke integration with a Crestron Control System also allowed remote control over the lighting at any time and was designed in house by SMC using Raytec's network lighting API.

OPTEX PIR's were installed to detect the first signs of an intruder and automatically trigger the Raytec Network Lighting as a



continue on page 53

first line of response to deter any potential intruders. Simultaneously the system sounds an internal alarm in the estate office and the manager's apartment.

The powerful LED lighting enables new Samsung PTZ network cameras to deliver high quality images during the hours of darkness, providing reliable information to the staff as to who or what is on-site. The security team are able to use the Crestron system via a simple touch screen interface to take live control over any individual illuminator or group of illuminators. Selecting them via a simple map view, they can flash key zones of illuminators in the exact place an incident is occurring as a further warning signal to deter crime.

Sean Gill, SMC Security Manager commented, "We selected the Raytec IP lighting as it could be easily integrated with the wider system and enables us to respond instantly to any potential break-ins, even if they occur out of hours. The high quality LED lighting is also crucial to helping our CCTV operate at night. We know that our PTZ cameras can zoom in on any incident anywhere in the grounds and capture exceptionally detailed images in the dark. In fact, the new IP system has already allowed us to prevent a potential break-in and helped us to clearly identify the intruders!"

"This is a fantastic example showing the endless integration possibilities with Network Lighting" commented David Lambert the Managing Director of Joint, Raytec. "IP lighting is fully customisable to any requirement and represents a leap in the performance capability of security systems. We're pleased that SMC have been able to use our API to create a bespoke lighting integration with their Crestron Control System which puts them firmly in control of their security at all times".

The installation has been an incredible success with proven results and the estate is extremely pleased with the final outcome. Both SMC and Raytec are pleased that their collaboration of intelligent system design and IP surveillance lighting has significantly improved security, actively prevented crime, whilst creating a flexible system that can adapt and evolve with the needs of the site.

For more information please visit www.smc-uk.com
SST

"We selected the Raytec IP lighting as it could be easily integrated with the wider system and enables us to respond instantly to any potential break-ins, even if they occur out of hours. The high quality LED lighting is also crucial to helping our CCTV operate at night. We know that our PTZ cameras can zoom in on any incident anywhere in the grounds and capture exceptionally detailed images in the dark. In fact, the new IP system has already allowed us to prevent a potential break-in and helped us to clearly identify the intruders!"

- Sean Gill, SMC Security Manager

Policing SMART Cities Around the World

Pittsburgh, Pennsylvania, USA

The NCFTA was established in Pittsburgh in 2002, as a neutral, trusted environment for companies, government, and academia to work together on identifying, mitigating, and ultimately neutralizing cyber crime threats globally.

Through the NCFTA, leading companies, subject matter experts, and strategic government agencies work side by side in a neutral environment to responsibly share cyber threat information in order to develop threat intelligence as part of an international effort to combat and defeat cyber crime. As partners, participating companies learn about cyber threats in real time and are able take proactive steps to mitigate and protect their systems, assets, data, reputation, and customers.

West Midlands, England, UK

Having faced the second largest funding fall of police forces in England and Wales under the Coalition Government, WMP realised they would not achieve their objectives for 2020 without redesigning their working methods. Shifting communications to online channels has already saved the force £5 million, while apps that allow officers to resolve tasks remotely will reduce the amount of time spent in transit.

Santa Cruz, California, USA

In Santa Cruz, California, police forces have successfully applied predictive analytics to burglary data to identify the streets at greatest risk and then increase patrols in those areas. The result has been a 19 per cent drop in property theft without deploying additional officers.

Dubai

Small self-driving cars will act as mobile surveillance units for the Dubai police by the end of 2017. First reported by the Gulf News, the vehicle is about the size of a children's toy car and is built by Singapore-based start-up OTSAW Digital. They're officially known as O-R3, and the company says that the Dubai police will use the robots to "fulfill low-level order enforcement tasks," which include scanning an area "for wanted criminals and undesirables." Capable of 360-degree surveillance, the bot comes with its own drone to further investigations. The O-R3 is the latest step in the move towards the digitization of surveillance.

India

The NASSCOM-affiliated Data Security Council of India (DSCI)sets up cyberlabs in different cities and imparts training. This model is now ripe for scale-up across the country and can be tapped into by the jurisdictional police.

Bangkok, Thailand

Bangkok's Metropolitan Police are upgrading their crime-fighting database with the help of the New York City Police Department, the first such cooperation between the NYPD and an Asian police force.

The NYPD developed its digital crime database and a unique crime-fighting management method known as CompStat, which maps past crimes and other related statistics and data. This helps the NYPD tackle crime more efficiently - something that the Bangkok force wants to emulate. The new data system will also allow the police to access non-police data such as rescue services or community group data and the digitisation of all such information should help shorten the time-frame for police response and deployment.

Singapore

Singapore's new "Safe City" pilot is a one-year programme where private sector companies work with the Government to integrate advanced analytic capabilities into the existing video monitoring systems used in the city. Should potential incidents be identified, alerts are sent instantly to the relevant authorities, including the police.

Victoria, Australia

Victorian officers will receive tablets in a bid to reduce time spent in the office filling out paperwork and allow frontline police to respond more quickly whilst on duty. The tablets will give officers more access to information about offenders and victims. Positive drug testing is now processed within 5 minutes rather than 30, with the officers able to process that information on the spot rather than return to their station.

AGT Leveraged the Internet of Things to Improve Attendees' Experience at Tomorrowland

With the rise in popularity of mega events, particularly music festivals in Europe and beyond, managing large-scale crowds and ensuring an enjoyable experience for attendees has become an increasingly difficult task for governments, event organisers and security personnel. At mega events such as Tomorrowland, Europe's biggest electronic dance music festival, it is critical that attendees can thoroughly revel in the experience and an exceedingly vital part of these events is to avoid disruptions and maintain a positive atmosphere.

More than 600 large music festivals take place every summer in Europe. Some of these mega events gather tens of thousands of music lovers and recent years have seen growing numbers in attendance. An increase in attendees leads to amplified crowd management and logistical issues that festival organisers need to address while preparing and managing the events.

This year, AGT International leveraged the Internet of Things to ensure a great experience for 60,000 party-goers who gathered each day during two weekends for Tomorrowland by harnessing publically available data across cloud-based platforms, such as social networking sites, blogs, video sharing sites and forums and applying advanced analytics to the data to create a comprehensive "map" of what was happening at the event. Effective management of the event was critical to event security and by using these technologies, we were able to create a safer, smoother and more pleasant experience for event participants and attendees.

The event, organised by the entertainment company ID&T Belgium, effectively used cutting-edge technology provided by AGT to improve situational awareness and manage potential disturbances before they even occurred. During the two weekends, we evaluated

continue on page 57

more than 1.4 million tweets and posts in 20 languages. Of that amount, 50 required investigations and a number of immediate interventions by the organisers or the police.

AGT International's CityMind 6.5 platform played a key role in ensuring that Tomorrowland was an enjoyable environment for festival attendees and the Event Control Center was larger than ever before. Here's a quick look at how our technologies were used throughout the event:

AGT integrated 220,000 SendRato bracelets with localisation information into our CityMIND solution as well as Zepcam body cameras and a full suite of social media monitoring using Tardis and OpenMIND. Leveraging an integrated data technology system pulling data from the bracelet system, event managers and Belgian police were able to evaluate potential incidents in real-time and direct emergency services and security guards to respond to incidents on the ground in a timely manner.

CityMIND provided a common operational picture of the event site with a cloud-based USAP. On the USAP, we were able to show crowd density in several layers with heat maps, which linked to the bracelets and social media posts. Teams of emergency responders, event organisers and security personnel were localised by their bracelets so that they were constantly visible on a specially created high resolution 3D map, providing a real-time situational overview.

> "The event, organised by the entertainment company ID&T Belgium, effectively used cutting-edge technology provided by AGT to improve situational awareness and manage potential disturbances before they even occurred."

Large events may continue to be a source of tension and an environment for potential disruptions, but "smart city" platforms running on the Internet of Things to leverage Big Data and Cloud Computing have already begun to transform how mega events are being managed.

As more information becomes publically available through social networking sites, blogs, video sharing sites and forums, mega event organisers and "smart city" solution providers – including AGT – are better understanding and more effectively managing potential disturbances at these events before they even occur. At AGT, we look forward to continuing to help improve the experience of attendees at these ever-increasing mega events around the world.

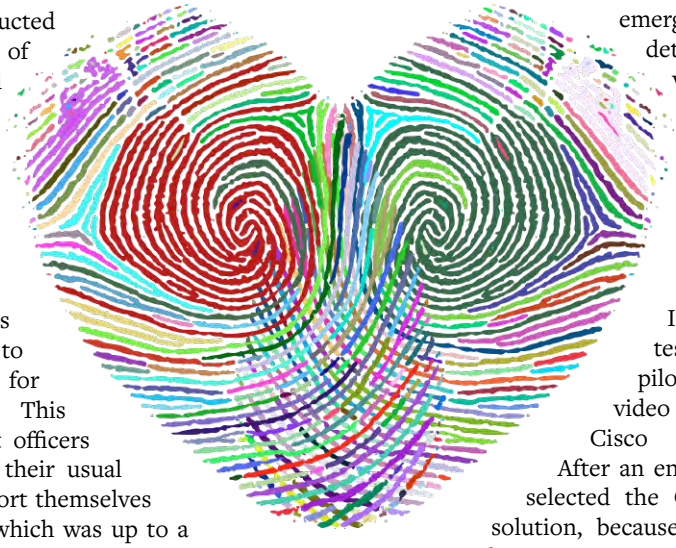
For more information, please visit: www.agtinternational.com SST

Prominent U.S. Police Department Redefines Collaboration Through Video

Suffolk County Police Department installs Cisco® video-conferencing capabilities to support officers and ensure public safety

Challenge

The Suolk County Police Department (SCPD), located in the State of New York, is one of the largest police departments in the United States. With approximately 2400 active officers that patrol more than 900 square miles, SCPD is responsible for protecting nearly 1.5 million people every day. Due to the department's large scale and reach, SCPD leadership has sought solutions to train its officers and manage all of its operations in a more efficient manner. To communicate important information to all seven precincts effectively, training officers would have to present the same information multiple times to ensure that it was received and understood—an overall time-consuming process.



SCPD traditionally conducted training a variety of ways. There would be instruction at a centralised location, monthly inspections, roll call and training videos that were viewed during an officer's administrative time. Most commonly, officers would have to travel to the police academy for mandatory trainings. This arrangement meant that officers were pulled away from their usual duties and had to transport themselves to the central location, which was up to a 45minute drive for some. For any additional training the department wanted to do in the precincts, it had to send trainers out to each area multiple times to offer sessions that worked with everyone's schedules and shifts. In fact, the department was sending its trainers out on average 35 times per training program, each lasting 6 months. This method of training proved inefficient and costly.

SCPD began to explore options that would ensure both all-force communications and training were offered in a way that was efficient and effective for both officers and the department. SCPD leadership decided on a solution that would modernise infrastructure and operations to reflect the growth of the county and the responsibilities of the department.

Solution

As SCPD began its search for a technology solution, it knew that it needed a platform that would enable quick and effective communication with its officers in the field, as well as improve its training program's efficiency. Keeping in mind that one of the biggest elements of police communication and training is face-to-face interaction, SCPD prioritised finding a solution that would allow officers to provide instant feedback on specific cues, movements, and facial expressions that are critical in responding to emergencies. Therefore, SCPD determined that a lifelike video platform would be the ideal solution because it has the potential to provide the same benefits as face-to-face communication, but without the travel.

In 2014, SCPD researched, tested and implemented pilot programs for various video platforms. One was the Cisco TelePresence® solution. After an entire year, the department selected the Cisco video-conferencing solution, because it is both high quality and easy to use something that was crucial to officers who, in the middle of an emergency, don't have time to troubleshoot technical failures. To complement this option, Cisco offered SCPD a multiphase rollout to its video capabilities so that the department can evolve over the next several years and officers can easily become familiar with the technology.

The first phase focused on establishing the technology in the department's infrastructure, which SCPD dubbed VIPER—Video Interactive Police Education Resource. SCPD procured Cisco TelePresence SX80 Codec units with the associated software and feature

continue on page 59

sets, as well as Cisco Business Edition 6000 on Cisco Unified Communications servers to enable the police department to have full control of a comprehensive set of tools and features available to customise their deployment. The department put large-scale monitors in its headquarters and installed two 70-inch high-definition (HD) screens in each precinct to enable instantaneous visual communication and collaboration.

SCPD also included customised audio sound bars from a Cisco partner to oer high-quality sound for each of the seven precinct deployments. Two additional units were deployed at police headquarters in Yaphank and the police academy in Brentwood, Long Island.

Phase two of SCPD's video solution will involve expanding the program beyond the department itself. It will increase recording capabilities to provide the ability to play back missed trainings or to create on-demand trainings officers can access any time. SCPD plans on spreading its video capability to its mobile command post in this second phase so that it can stream video from mobile locations, such as the squad cars, back to headquarters.

Results

VIPER has been a huge success for SCPD. The VIPER program helps to improve the administration of the Suolk County police force by using innovative video conferencing throughout the 900-plus square miles of the county. VIPER reduces administrative costs for travel between precincts and headquarters, and allows all officers to be trained in a time effective manner. Communications across the entire force have improved so that officers can operate more efficiently and strategically.

Department leadership has received positive feedback from officers, particularly about the large-scale monitors in each precinct. The solution has enabled timelier and more consistent communications with officers not only with each other in each precinct but also with personnel throughout the county as well. Oftentimes, the information that leadership needs to convey from headquarters to precincts is time sensitive and mission critical. The new system ensures information is delivered clearly and quickly for the problem to be addressed. Having all communications and training originate from one source has helped avoid confusion and miscommunication among SCPD officers, ultimately allowing the entire police force to operate as a more cohesive unit.

In terms of training, the department has seen both cost and time savings. While SCPD still does send trainers in person to precincts, Cisco TelePresence technology has drastically reduced the amount of times the trainer is in the field. Now the department sends a trainer into

> "After an entire year, the department selected the Cisco video-conferencing solution, because it is both high quality and easy to use something that was crucial to officers who, in the middle of an emergency, don't have time to troubleshoot technical failures. To complement this option, Cisco offered SCPD a multiphase rollout to its video capabilities so that the department can evolve over the next several years and officers can easily become familiar with the technology."

continue on page 60

the field only four or five times per program—a huge source of cost savings for the department. Additionally, the courses that previously ran for 6 months are taking about 2 weeks to complete.

Thanks to its new virtual communication tool, police officers that were previously occupied or away from their stations are now onsite, equipped and prepared for any situation. Also, the department and its trainers are saving significant amounts of time and money by streamlining processes. Overall, the increased training and improved communications that VIPER has facilitated means that SCPD has enhanced its training and Suolk County citizens are reaping the benefits.

Next Steps

While phase one of SCPD's video solution has been rolled out and is completely operational, phase two will add even more functionality to the department. SCPD will be able to reach outside its own precincts and externally communicate to any department or resource it would like to bring into their video network, such as the U.S. Department of Homeland Security or the district attorney's office. This integrated level of communication further defines SCPD's role in national public safety and will provide Suffolk County residents with an even higher level of protection and support.

SCPD is also looking at smaller desktop units such as the Cisco DX70 and DX80 to be placed with its commanders and high-ranking officials in the department, so they can instantaneously communicate with each other with video. Additionally, SCPD is interested in spreading live video feeds from its video-conferencing system to its mobile command posts and even helicopters.

"Thanks to its new virtual communication tool, police officers that were previously occupied or away from their stations are now onsite, equipped and prepared for any situation. Also, the department and its trainers are saving significant amounts of time and money by streamlining processes. Overall, the increased training and improved communications that VIPER has facilitated means that SCPD has enhanced its training and Suolk County citizens are reaping the benefits."

Eventually, SCPD would like to see the video-conferencing technology implemented at five east-end town agencies to help them operate in a more interconnected manner. It also wants to expand the technology to the county's Office of Emergency Management to more easily share information during an incident.

For more information, please visit: www.cisco.com SST

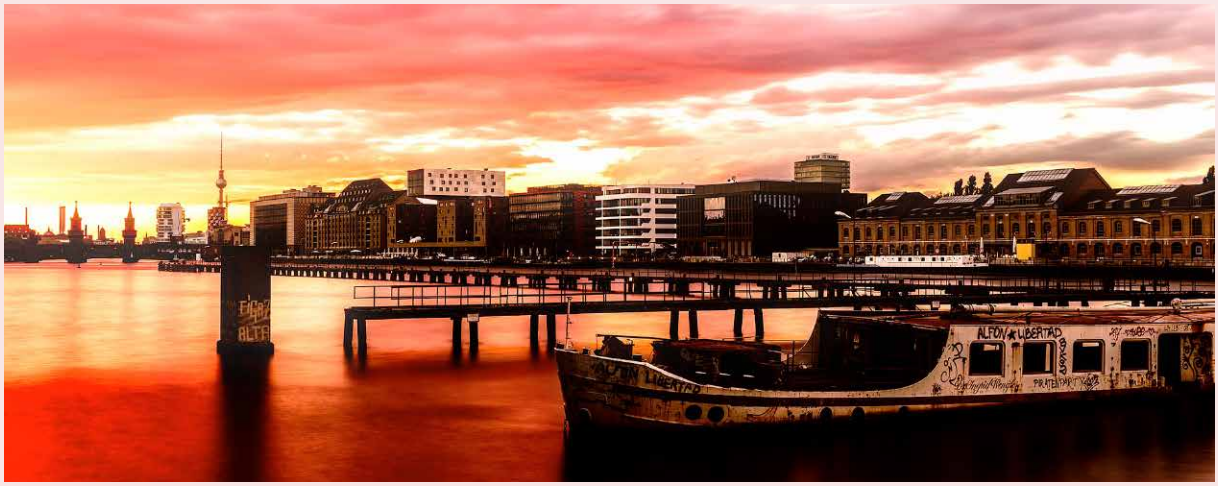
Canary Wharf Group Heightens Security with Unified Platform by Genetec

Canary Wharf is one of the busiest business and financial districts in London, England. Its team upgraded its security system to Genetec Security Center, unifying IP video surveillance, access control and automatic license plate recognition under one platform.

The Company

Canary Wharf is one the busiest business and financial districts in London, England. It offers over 14 million square feet of office and retail space on 97 acres, and welcomes over 140,000 people daily. Many major banks, professional services firms and media organizations, including Barclays, Credit Suisse, HSBC, J.P. Morgan have their global or European headquarters within the bustling district. Canary Wharf Group, a fully integrated

continue on page 61



property development and management company, caters to every aspect of the district's high-quality needs, including security.

The Challenge

Canary Wharf had been running an old analog DVR-based video system, which was unreliable, difficult to scale, and lacked flexibility. Their team was ready to move to IP and wanted a system that could be used with many different technologies, and accommodate standard IT practices.

According to Mike Walker, Security Technology Manager at Canary Wharf Management Ltd., "Our job is to ensure it's always business as usual. We're managing a mini city, and we want people to feel comfortable and secure without being invasive. It's all about finding that balance."

> "Why have separate systems when you can have it all in one? All of the information we need is available from one central platform."
>
> ***- Bernadette Bashford-Payne, Estate Control Center Manager, Canary Wharf***

Results

Canary Wharf has implemented the IP video surveillance, access control and ALPR system within the Security Center, unified platform. Operators work from a map of the district to easily respond to alarms, pull up cameras, lock and unlock doors, and track suspects. Canary Wharf actively works with the police and credits the unified security platform with streamlining communication with government agencies.

Canary Wharf is also using the unified platform for operational benefits. From a business standpoint, Security Center is helping to retain and attract their many prestigious clients. "When we bring potential clients through our control room, the system provides the wow factor that helps us sell our business district. This system helps us convince our clients how secure they will be here, and how efficient our security team is," said Mike Walker.

The Solution

Unified Security View
The team at Canary Wharf manages all security systems from the unified platform, and quickly responds to events from a map-layout of the business district.

Secure Collaboration
High-ranking security team members can remotely access or securely share video with authorities using highly-secured encryptions and other security tokens.

Vehicle Tracking Made Easy
The team tracks vehicles within the business district by using the AutoVu automatic license plate recognition system which automatically notifies police of hotlist hits.

Operational Improvements
Retrieving video archives to review how events were handled helps management and other agencies improve response processes.

Products Used

AutoVu™
The AutoVu™ automatic license plate recognition

continue on page 62

(ALPR) system automates license plate reading and identification, making it easier for law enforcement and for municipal and commercial organisations to locate vehicles of interest and enforce parking restrictions. Designed for both fixed and mobile installations, the AutoVu system is ideal for a variety of applications and entities, including law enforcement, municipal, and commercial organisations.

Omnicast™
As part of the Security Center unified platform, the Omnicast™ IP video management system (VMS) provides organisations of all sizes the ability to deploy a surveillance system that addresses their unique video security needs. Through deep support for a wide range of industry-leading cameras, encoders, and CCTV equipment, the Omnicast system scales and adapts to the changing demands of your security environment.

Synergis™
The SynergisTM IP access control system (ACS) heightens the security of your organisation and increases your readiness to respond to incidents and threats, all while leveraging any existing network and security equipment investments. With advanced security measures and support for an ever-growing number of 3rd party access control devices, the Synergis system gives you the confidence to protect your people and assets.

Plan Manager
Plan Manager is a module of Security Center offering interactive and graphical mapping to better visualise and manage security environments. With the ability to dynamically navigate through facilities and oversee a greater number of cameras, doors, automatic license plate recognition (ALPR) cameras, intrusion, and other security applications, Plan Manager provides complete and real-time coverage from small to large multi-site environments.

> "Operators work from a map of the district to easily respond to alarms, pull up cameras, lock and unlock doors, and track suspects. Canary Wharf actively works with the police and credits the unified security platform with streamlining communication with government agencies"

Security Center
Security Center is the unified security platform from Genetec™ that blends IP security systems within a single intuitive interface to simplify your operations. From access control, video surveillance, and automatic license plate recognition to communications, intrusion, and analytics, Security Center empowers your organisation through enhanced situational awareness, unified command and control, and connectivity to the cloud. SST

Dahua Technology Showcases Strength in Safeguarding 9th BRICS Summit

Hangzhou, China - The 9th BRICS Summit was successfully held in Xiamen, China from the 3rd to the 5th of September, where national leaders of the five member countries were in attendance. Building on its success in providing a comprehensive security solution for the G20 Hangzhou Summit in 2016, the 9th BRICS Summit was yet another accomplishment for Dahua.

In partnership with the BRICS Summit security team, Dahua constructed a robust security barrier, guaranteeing a smooth opening for the summit.

Dahua Secures Key Summit Areas

Dahua provided comprehensive security coverage in the following key areas:

Main Meeting Venue and Surrounding Areas

The BRICS security command center, administered by the Public Security Department of the Xiamen, was fitted with a Dahua visual emergency dispatch and command system. The Center's large display wall was stitched together with Dahua edgeless HD LED panels, enabling a complete picture of all units under command center control during the meeting, greatly simplifying control and responses.

Dahua Edgeless HD LED

Main BRICS Venue

The security system surrounding the Xiamen International Conference and Exhibition Center as well as the visual emergency dispatch and command system in the security command center both adopted a full range of video surveillance and display solutions from Dahua.

Dahua Video Surveillance Systems Safeguarding Xiamen International Conference & Exhibition Center

Police Cars

A customised Dahua Mobile Solution with GPS positioning and in-vehicle wireless image transmission system was installed on 228 patrol cars and 72 special cars from the Xiamen Public Security Bureau which was used to clear the way for Summit leaders. This provided the command center with a continuous live overview

of all areas while providing support for the handling of various emergencies.

Customised Dahua Mobile Solution Installed on Xiamen Police Cars

Key Routes in Xiamen's "Four Bridges and One Tunnel" Road Network

"Four Bridges and One Tunnel" is the phrase used to describe the various road access points to Xiamen Island, the location of the main Summit venue. In order to secure these access points, Dahua employed advanced technologies such as intelligent analysis, big data, and video analysis centers to significantly increase the efficiency of emergency command and information technology management capabilities, providing uninterrupted HD video surveillance and smart road event monitoring on bridges and tunnels. This ensured smooth operation of each component in the "Four Bridges and One Tunnel" and prevented disturbances during the BRICS Summit.

> "The security system surrounding the Xiamen International Conference and Exhibition Center as well as the visual emergency dispatch and command system in the security command center both adopted a full range of video surveillance and display solutions from Dahua."

continue on page 64

Dahua Advanced Technologies Employed in "Four Bridges and One Tunnel" Control Center

In addition, Dahua also contributed to the security of other key areas including the Xiamen Airport, train station, ferry piers, and police checkpoints.

Dahua Intelligent Solutions Applied on Key Routes from Xiamen Airport to Main Meeting Venue

> "In order to secure these access points, Dahua employed advanced technologies such as intelligent analysis, big data, and video analysis centers to significantly increase the efficiency of emergency command and information technology management capabilities, providing uninterrupted HD video surveillance and smart road event monitoring on bridges and tunnels. This ensured smooth operation of each component in the Four Bridges and One Tunnel and prevented disturbances during the BRICS Summit."

Hotel Areas

In surrounding Haicang and Jimei districts, Dahua constructed video surveillance on routes and sites which held key activities in the city, achieving full coverage of places such as guarded routes, main roads, key sites, as well as surrounding areas and regions of elevated-risk.

Dahua Video Surveillance Solution applied in Hotel Areas

Dahua also played a role in safeguarding conference-related affairs such as catering, accommodation, and travel. The hotels in which leaders stayed in and surrounding areas were upgraded to HD systems in a short amount of time, making sure the leaders were secure while they rested during the Summit. The mobile law enforcement surveillance system assisted the Xiamen Market Supervision Commission in guaranteeing the provision of safe food during the Summit. The Dahua Smart Healthcare Solution covered various grade-A hospitals in Xiamen, enabling them to be ready for possible emergencies at any time. Dahua also participated in logistics services during the Summit.

Beautiful Xiamen in the "Eyes" of a Dahua Camera

Since January, Dahua had been actively engaged in the Summit's surveillance operations. During the security deployment period, with its advanced technologies and dedicated man-power, Dahua assisted the city's public security and traffic police departments in accomplishing almost 300 security tasks and ensuring zero device malfunctions during the Summit. Summit security units have spoken highly of Dahua's rigorous and practical attitude, strictly standardized operations, and intelligent video surveillance solutions. SST

Smart City Improves Public Security Efficiency

Background

The city of Langfang, Hebei province, located between Beijing and Tianjin, is known as the "Jewel in the Beijing-Tianjin Corridor." As the only passage to Beijing from the south, Langfang requires public security protection. To address challenges brought about by its rapid economic development, the Langfang police department and Huawei started working together on a project to develop the city's video surveillance system.

Huawei made a thorough analysis of Langfang's progress in ICT, and recommended a "Smart City" solution. After several rounds of high-level communication and visits, the Langfang municipal government signed a strategic cooperation agreement with Huawei in 2011 to build a "Smart Langfang." In the same year, Huawei developed Smart City ePolice and checkpoint systems for Langfang.

In February 2012, Langfang decided to upgrade its existing video surveillance system to an HD digital system. Huawei then invited the customer to visit its "Safe City" showcase in Kunming, Yunnan province. Following in-depth communication, meticulous studies and comparisons, Langfang's municipal government and police department selected Huawei to provide the technical design of Langfang's safe city project. Huawei won the project over a number of competitors with its advantages in technical strength and solution design.

Challenges

Langfang's previous video surveillance system did not provide unified management. In addition, images taken by SD cameras were not clear enough to effectively help investigations.

Another problem was that the old platform could not efficiently protect recorded data. Incidents of video loss occurred from time to time.

The lack of intelligent analysis services led to the following problems:

- Manual browsing of surveillance videos was very time-consuming for large numbers of personnel.
- Even if a digital video system was operating normally, the system could not detect a faulty analog camera. When an incident occurred, police would find that the relevant analog surveillance video was blurry, damaged, or even had not been recorded.

The customer needed a new platform with higher quality video capabilities including diagnoses in order to improve system maintenance. The new platform required detection of image quality exceptions such as image loss, blue screen, frame freezing, and mosaic.

Solution

Huawei provides "Smart Langfang" with an end-to-end solution: a platform integrated with software, servers, storage units, network, cameras, and decoders. Huawei's HD camera uses a second-generation Exmor CMOS chip that features back-lit sensor technology. A large-capacity back-end ISP and Huawei-proprietary coding algorithm secures Huawei's leading position in the camera industry.

The new platform supports the GB/T28181 protocol, which permits integration with the existing platform and unified management for all network elements.

The integrated hardware architecture enables every hardware unit to store, distribute, and forward data streams, thus minimising the number of faulty points. The platform provides cluster deployment and two-level security protection for data on the hard disk and host layers, preventing video data loss.

The platform also enables timely maintenance with intelligent video quality diagnosis functions that detect image exceptions and generate relevant log reports. When an exception occurs, the system automatically

continue on page 66

generates an alarm to notify on-duty personnel of the need for inspection.

Benefits

The highly scalable "Smart Langfang" system enables large-scale expansion for the future. Now, the new system covers all key areas in the city, substantially improving public security, and raising case investigation efficiency by more than 20 percent.

Intelligent video quality diagnostics facilitate work force distribution, improve security efficiency by 30 percent, and enable 24/7 video surveillance services.

The Langfang Safe City system has 3,000 surveillance sites, which is still not enough to cover the entire city. To ensure the city's security protection needs and promote social and economic development, the Langfang municipal government plans to expand the system to cover all subordinate districts, at a market value of up to USD $50 million to $70 million. SST

Safety a Priority for Toronto Community Housing

There aren't very many environments more challenging to secure than 400 high-rise apartment buildings and townhouse complexes spread across one of the largest cities in North America. Toronto Community Housing is the largest social housing provider in Canada and the second largest in North America. Wholly owned by the City of Toronto and located in 106 of the city's 140 neighborhoods, the apartment buildings and townhouse complexes are home to more than 110,000 people.

With so many properties spread so widely around the city, a reliable, effective video surveillance system is of critical importance in providing residents with clean, safe, well-maintained and affordable homes, which is Toronto Community Housing's core mission.

The organisation began deploying March Networks® video surveillance technology more than a decade ago and currently has in excess of 500 video recorders and approximately 8,000 cameras capturing video at strategic locations in and around its buildings.

Toronto Community Housing's surveillance model was originally decentralized, so when an incident occurred, a member of the Smart Buildings and Energy Management (SBEM) team would have to drive out to the site to review and export video. "Not all of the buildings were networked together, so it was difficult to manage," said Boyd Dyer, SBEM-Facilities Team Director.

However that's changing. Beginning earlier this year, Toronto Community Housing began upgrading its network and rolling

continue on page 67

> "In the past, it was the responsibility of site staff to check their system and bring any issues to the attention of Dyer and his team. Now, camera outages, network failures and hard drive issues are detected by the health monitoring functionality in Command™ Enterprise and brought to the attention of system administrators in the health inbox or via email alerts."

out March Networks Command Enterprise video management software. It's also in the process of transitioning to March Networks 8000 Series Hybrid Network Video Recorders (NVRs) and third-party IP cameras.

As sites are connected, Dyer's team members are able to configure video recording parameters, set user privileges, access health alerts, view video and export clips without having to leave their office. Staff of Toronto Community Housing's internal security department, the Community Safety Unit, also have access to the system and can export video footage for law enforcement purposes.

"The ability to review video and manage the system on a centralised basis means we don't have to drive all over the city, so it speeds investigations and saves time," said Dyer.

Making sure that more than 500 video recorders and 8,000 cameras are operating at peak performance is especially important. In the past, it was the responsibility of site staff to check their system and bring any issues to the attention of Dyer and his team. Now, camera outages, network failures and hard drive issues are detected by the health monitoring functionality in CommandTM Enterprise and brought to the attention of system administrators in the health inbox or via email alerts.

"My team is responsible for the upkeep and maintenance of the system, so we'll triage the problem and dispatch one of our staff or our security systems integrator to rectify it," said Dyer.

Camera tampering is a common occurrence and needs to be addressed expeditiously. "It happens frequently," said Dyer. "That's one of the reasons we're so busy."

Using the Command Enterprise mass management functionality, Dyer can schedule recorder configuration settings, firmware updates and device settings at his preferred time to minimise the impact on network bandwidth. The software also supports multiple video streams for efficient use of bandwidth and storage, and allows for customisation of the user interface.

If staff, for example, are only tasked with accessing and reviewing video, the Command Client user interface can be tailored to their specific needs. They only see the features and functions they need to perform their job without the distraction of additional capabilities they will never use.

This helps with training, said Dyer. "Not everyone needs to be trained to the same level. Site staff, for example, just need to see the cameras. Internal security staff need to both review video and extract it, whereas my staff need to know how to administer and configure the system."

In a busy environment with hundreds of sites and no shortage of reported incidents, no one has the time to spend hours reviewing archived video. Using Command Enterprise, Toronto Community Housing staff can quickly zero in on evidence using the software's Visual Finder and Motion Histogram tools. The Visual Finder allows users to speed through the timeline to the date and time of an incident, while the Motion Histogram pinpoints video corresponding with increased activity in the field of view.

The transition to March Networks 8000 Series Hybrid NVRs provides Toronto Community Housing with a powerful and versatile recorder. Featuring an embedded

continue on page 68

Linux-based operating system, 32 channels of video and up to 32 TB of internal storage, the 8000 Series NVRs offer industry-leading reliability and archiving capacity for high-definition video.

The recorder's internal battery backup guarantees a systematic shutdown in the event of an unexpected power loss, while hard drive mirroring ensures storage redundancy.

Toronto Community Housing is also likely to save money on service calls thanks to the QR codes on the 8000 Series recorders, which work with the company's industry-first GURU Smartphone Application to help technicians quickly diagnose issues, confirm warranty status, run installation reports, conduct security audits, process express return merchandise authorisations and access video tutorials using their smartphones or tablets.

In Dyer's experience, however, March Networks recorders excel in reliability. "We rarely have problems with them. The failure rate is very low," he remarked.

The biggest beneficiaries of video surveillance at Toronto Community Housing are the residents, who appreciate the deterrent effect it has on crime and how it helps create a safe environment.

"The residents are big fans of video surveillance and regularly let our site staff know when they see that a camera has been dislodged or tampered with," said Dyer.

The lightning-fast resolution of a shooting incident last summer is a perfect example of the value of Toronto Community Housing's video surveillance system.

> "The residents are big fans of video surveillance and regularly let our site staff know when they see that a camera has been dislodged or tampered with,".

"The incident happened in the morning and by the afternoon the suspect was in custody," recalled Dyer. "We had a high-definition camera in the location and the recording was crystal clear. We pulled the video, gave it to police and they recognised the individual right away.

"Residents feel safer knowing that if something like this happens, it will be investigated and resolved. Like any other community, the majority of people living in Toronto Community Housing are good people, and in a lot of cases, it's people coming onto our properties from outside who are causing trouble."

For more information, please visit: www.marchnetworks.com SST

Public Safety with Milestone South Korea's Smart City Ensures Public Safety with Milestone Video Surveillance Solutions

City Challenges

The city of Goyang, named one of the 10 most dynamically developing cities in the world, is located 20 minutes northwest of Seoul, in the Gyeonggi Province in South Korea. Home to Seooreung, a UNESCO World Heritage Site, the city has a rich 600- year history and attracts plenty of tourists throughout the year. To ensure

continue on page 69

a safe and enjoyable experience for visitors, the city sought an experienced and reliable vendor to maintain security.

The city's previous video surveillance system often experienced downtime and required a manual reboot each time it failed to function efficiently. The technical team that supported this project was under tremendous pressure and under- resourced, which meant that issues could take two weeks before being resolved. The old video management software also had several flaws. It required constant monitoring by numerous staff members and generated high maintenance costs from the lack of support for HDTV cameras. Goyang sought to improve the quality and reliability of their video surveillance system, and more effectively crack down on crime-prone districts and blind spots in the city.

Integrated IP Video Solution

Milestone first did a comprehensive 360-analysis of Goyang's existing security needs, before recommending an improved IP video management system to keep the public safe. In November 2014, Goyang worked with Milestone Platinum Partner, Omecca, to replace the old local video management software with Milestone XProtect video management software. The existing hardware environment, including the network attached storage (NAS) equipment from Milestone Technology Partner EMC Isilon, was retained for optimal archiving of the video data.

The previous software managing the city's 2,500 video cameras was replaced in under two weeks without causing any disruption to daily operations. In addition, two new software applications were integrated with Milestone's open platform architecture: a facility management system and another third-party software for remotely exporting videos. Both solutions were developed in this impressively short period of time - a clear indication of Omecca's leading expertise with the technology.

The Advantages

In recent years, local governments in Korea have implemented surveillance centers to ensure public safety, and Goyang is no exception. With 2,500 cameras in the city now managed by the world's leading video management software from Milestone, Goyang is safer than ever. For system operators Milestone XProtect software is easy to learn and use, with each staff member able to monitor about 100 cameras simultaneously thanks to the carousel feature and comprehensive XProtect Smart Wall overview.

The scalability, flexibility, reliability and cost-effectiveness of the IP-based Milestone VMS have also brought other significant benefits to Goyang. The open interoperability designed by Milestone Systems enables installing partners to implement best-in-class solutions for customised, enhanced security. This provides a future-proof platform that is scalable and allows integration with new innovations in security as they become available.

Public Safety: The Top Priority

The city of Goyang is located approximately 20 minutes north of Seoul with a population of just over a million. The city has become an exemplary leader in the country in many areas such as economic vitalisation, numerous friendly residential areas, and modern transportation

> "Public safety remains our number one concern. Upgrading our video surveillance infrastructure allows us to better monitor the city streets, especially our crime-prone districts and previous blind spots. Implementing an IP video surveillance solution based on Milestone's platform was a major improvement."
>
> ***- An Dong Soo head of Civil Safety Center, Goyang City***

continue on page 70

systems. Selected as one of the "World's most dynamically developing top 10 cities" by Newsweek, Goyang City has made the safety of its residents a priority. The city has installed over 2,500 cameras to date. In order to monitor such a large number of cameras effectively, Goyang needed a flexible, scalable and reliable video management software. Goyang's old systems were outdated and had stability issues, often experiencing downtime which required external technical teams to x. In addition, their video software lacked scalability, as it only supported 25 channels per recording server, which led to high maintenance costs forcing Goyang to purchase many servers in order to ensure safety coverage of its citizens. As a result, Goyang turned to Milestone Systems to fulfill their new and long-term video management software needs. Milestone's cost-efficient and comprehensive video management software was easily implemented and employed by Goyang's security team.

"Public safety remains our number one concern. Upgrading our video surveillance infrastructure allows us to better monitor the city streets, especially our crime-prone districts and previous blind spots. Implementing an IP video surveillance solution based on Milestone's platform was a major improvement," explains An Dong Soo, head of civil safety center, Goyang City.

Goyang managed to replace their existing video surveillance software thanks to Milestone Platinum Partner Omecca installing Milestone XProtect in less than two weeks, without any disruptions to day to day service.

"The ability to install flexible, scalable Milestone software on our existing hardware infrastructure, and subsequently to add new features from interoperability with facility management software and remote video exporting, has helped us make continual improvements in the quality of our video surveillance technology," said An.

Reliability and Performance – A Necessity

Goyang City Hall runs a 24-hour security system that requires instant and easy access to surveillance video, and reliability is a core requirement. With Milestone XProtect, city employees have reliable video access, thanks to failover recording servers, and protection against the deletion or tampering of video data.

"Milestone's open platform IP video management software has helped us simplify our daily operations. Our security staff have access to uninterrupted video recording, and through the use of scheduled and event-driven rules in the Milestone engine, we have an easy way to automate security alerts and actions, also to control external systems and devices, reducing tasks that have to be done manually," comments An.

"Goyang City Hall runs a 24-hour security system that requires instant and easy access to surveillance video, and reliability is a core requirement. With Milestone XProtect, city employees have reliable video access, thanks to failover recording servers, and protection against the deletion or tampering of video data. "

In addition, Goyang has optimised system management with Milestone XProtect software. It provides real-time overview of system performance with a customisable dashboard, instant notifications regarding server problems and predictive video retention warnings with System Monitor, enabling Goyang to seamlessly adjust the data load on recording servers, moving cameras easily from one server to another in runtime with minimal interruption to the video stream, and without having to reconfigure cameras.

Open Platform Provides Flexibility

Milestone's open architecture also provides Goyang with the scalability and flexibility required to expand on the security with more innovations at any time. In addition to replacing the previous video management software, Omecca also developed and integrated two pieces of software – a facility management system to manage IP camera devices on site, and a video export software application for remote searching/playback/export of video data from other locations. The integrated monitoring system based on Milestone XProtect helps operators to respond rapidly to unfolding events. As the many cameras capture input from different angles, it gives system operators options to track live events. It is also easy to search recorded video to retrieve, bookmark and export evidence in case of crimes, and then share this information with the police to help resolve incidents.

"Video surveillance is rapidly developing today, and the flexibility of Milestone XProtect allows us to customise our video surveillance system, while enabling us to integrate additional applications for extra features," says An. "It also provides a reporting tool, which helps us

continue on page 71

track and understand the severity of incidents, and how we have helped in this process."

Planning for the Future

Since the initial installation in November 2014, Goyang City has added more than 1,000 new cameras every year. Goyang currently operates more than 4,700 citywide. With endless integration possibilities, Goyang is able to integrate and embed third-party applications and business systems into the Milestone software and XProtect Smart Client, through the Milestone Integration Platform (MIP).

"As the city continues to grow, we remain con dent that the Milestone security surveillance system can be easily expanded to accommodate additional security demands. Public safety is of paramount importance, and we are committed to investing in the latest technologies to help us reduce administrative time and improve the efficiency of our resources," comments An.

For more information, please visit: www.milestonesys.com SST

Safer and More Attractive Streets: Supporting the Evolution of Cities With ICT

Realisation of Smart City Solutions

With support for planning, design, and implementation of Smart City solutions in major cities around the world, NEC is contributing development of safe, secure, and attractive cities.

When "Smart City" was proposed as a new concept for urban development, it was considered by people primarily as environmentally-friendly urban planning that leverages information and communications technologies (ICT) to conserve resources. However, in recent years, as people continue to concentrate in cities around the world, Smart City solutions have broadened to include the intelligent use of ICT to prevent crimes and control traffic.

Seeking to realise sustained economic development while protecting the environment and ensuring people's safety and security-this is the goal of the Smart City projects that are being carried out worldwide. NEC is contributing to attractive urban development that brings about safe and comfortable lives for urban residents around the world by leveraging ICT assets such as the Internet of Things (IoT), image analysis, and cloud computing technologies.

As populations concentrate in cities, traffic control and public order become even more important

continue on page 72

> "Cities like Tigre in Argentina and Surat in India are seeking to create safe and secure communities by establishing departments within the police force that are dedicated to improving public safety by using advanced ICT."

Rapid urbanisation is taking place on a global scale. As a result, traffic congestion, environmental pollution, and public disorder are becoming even more serious issues. The growth of organised crime such as terrorism is also a cause for grave concern.

In response, many countries around the world have launched Smart City projects with achievement targets based on these issues. Specifically, what is being sought is urban development that not only reduces the environmental impact on the entire city by using resources wisely, but also creates new social infrastructure that leads to crime prevention and reduction of traffic accidents. This is urban development that ensures the safety and security of residents, improves their quality of life, and makes sustained economic development possible.

In this way, the concept of Smart City solutions is expanding from "smart energy" to "smart mobility" and "smart governance," and furthermore, to "smart security." What is demanded of ICT vendors is the provision of solutions that address the substantive issues faced by administrative agencies in each country.

NEC is the partner selected by three cities in Oceania, South America, and South Asia

Wellington, the capital of New Zealand, is seeking to become a safe and smart city fit for future generations with its "Wellington 2040" strategy, which makes use of cutting-edge technologies. One of the initiatives of "Wellington 2040" is the launch of a project to use ICT to comprehend the flow of vehicles in the city and understand their types. The purpose is to gather and analyse massive data sets of vehicle travel and reflect the results in urban development and road maintenance plans.

This project is using diverse sensing technologies and advanced analytic technologies to alleviate congestion and provide rapid response during emergencies such as car accidents, as well as provide efficient route navigation by accurately predicting traffic volume. The city government is expecting this project to provide a wide range of benefits, including appropriate road maintenance and effective securing of road space during urban development.

Cities like Tigre in Argentina and Surat in India are seeking to create safe and secure communities by establishing departments within the police force that are dedicated to improving public safety by using advanced ICT. In Tigre, the system the police are using is an urban surveillance system based on NEC's Face Recognition technology. This system can quickly search for criminal suspects and missing persons by matching in real time massive amounts of image information taken by numerous cameras installed in the city with a database of registered face photos.

The same system also employs cutting-edge functions to assist the police in maintaining order. These functions include "detection of two riders on a motorcycle," often associated with purse-snatching incidents, and "detection of riding without a helmet" for the purpose of providing safety guidance. Other technologies used are Number Plate Recognition and Behavioral Analysis to quickly identify suspicious vehicles and Crime Map Generation, which displays locations of past crimes.

By using these functions, the cities of Tigre and Surat can quickly comprehend potential dangers and trouble spots and address them to prevent crime. In Tigre, marked improvements have resulted, with car thefts reduced by about 40 percent.

continue on page 73

> "NEC is contributing to attractive urban development that brings about safe and comfortable lives for urban residents around the world by leveraging ICT assets such as the Internet of Things (IoT), image analysis, and cloud computing technologies."

Continuing to contribute to the realisation of an administrative infrastructure for a new era as a partner using advanced technologies

In recent years, competition among international cities to attract tourists and businesses has become fierce. In short, cities around the world are pressed by the need to maintain even safer and more secure infrastructure for not just their citizens, but also tourists and business travelers. It is also essential that cities improve their overall level of attractiveness by making the maximal use of their limited budgets.

As an ICT vendor possessing advanced technologies in all areas of computing, networking, and security, NEC will continue to contribute to the realisation of city and government infrastructures fit for future generations from the twin standpoints of providing safety and security and providing efficient services. NEC seeks to continue to be the partner of choice for customers around the world in the use of advanced technologies that support the realisation of Smart City solutions.

For more information, please visit: www.nec.com SST

NEC Deploys Smart City Solutions

Rapid urbanisation is a global phenomenon that is producing traffic congestion, environmental damage, worsening security and a host of other problems. Efforts are underway in countries around the world to make life safer and more secure for urban residents.

For example, the cities of Tigre in Argentina and Surat in India have recently deployed the urban surveillance systems based on NEC's Face Recognition technology to improve the safety and security of these cities. In Tigre, these systems use highly accurate Face Recognition to help police track down criminals and investigate crimes, Behavior Analysis to identify suspicious vehicles and dangerous driving that could lead to accidents and Number Plate Identification to swiftly identify fleeing cars. By quickly detecting potential risks and problems, these systems are designed to prevent crimes.

continue on page 74

"In Tigre, these systems use highly accurate Face Recognition to help police track down criminals and investigate crimes, Behavior Analysis to identify suspicious vehicles and dangerous driving that could lead to accidents and Number Plate Identification to swiftly identify fleeing cars. By quickly detecting potential risks and problems, these systems are designed to prevent crimes. "

NEC is planning to offer its Smart City solutions to cities around the globe, and promises to provide a range of services from operations planning to actual solution implementation. These initiatives contribute to the evolution of cities, make cities more agreeable and attractive places to live and help provide a better quality of life for everyone.

Supporting a National Project in India Through Advanced Recognition Technologies

India continues to exhibit rapid development spurred by its high economic growth. In order to equally provide education, healthcare, social welfare, and other social services to all residents, a Unique Identification Authority System for identifying each and every citizen has been launched in this country with a population of more than 1.2 billion.

Central to this initiative is an unprecedented, large-scale biometrics system for distinguishing 1.2 billion people, which is equivalent to approximately one-sixth of the world's population. The system collects biometric data, including fingerprint, face and iris data, and combines it to match and identify individuals. This enables issuing a unique ID to each and every citizen throughout India.

NEC built a highly reliable system by utilising the latest technologies in the continuously evolving field of biometrics, such as Face Recognition and Fingerprint Identification. NEC strongly supports the building of societies where people around the world can receive equal treatment and live in prosperity.

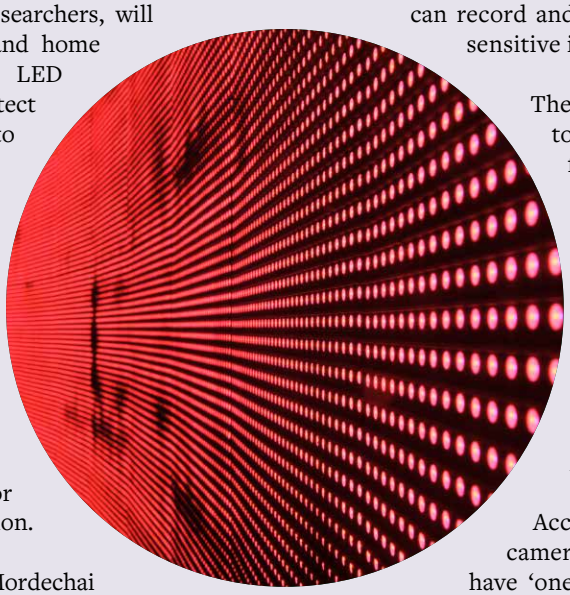
For more information, please visit:
www.necam.com SST

Security Cameras Can Be Infiltrated for Malicious Attacks by Using Infrared Light, According to Ben-Gurion University Cyber Researchers

Ben-Gurion University of the Negev (BGU) researchers have demonstrated that security cameras infected with malware can receive covert signals and leak sensitive information from the very same surveillance devices used to protect facilities.

The method, according to researchers, will work on both professional and home security cameras, and even LED doorbells, which can detect infrared light (IR), not visible to the human eye.

In the new paper, the technique the researchers have dubbed "aIR-Jumper" also enables the creation of bidirectional, covert, optical communication between air-gapped internal networks, which are computers isolated and disconnected from the internet that do not allow for remote access to the organization.



The cyber team led by Dr. Mordechai Guri, head of research and development for BGU's Cyber Security Research Center (CSRC), shows how IR can be used to create a covert communication channel between malware installed on an internal computer network and an attacker located hundreds of yards outside or even miles away with direct line of sight. The attacker can use this channel to send commands and receive response messages.

To transmit sensitive information, the attacker uses the camera's IR-emitting LEDs, which are typically used for night vision. The researchers showed how malware can control the intensity of the IR to communicate with a remote attacker that can receive signals with a simple camera without detection. Then the attacker can record and decode these signals to leak sensitive information.

The researchers shot two videos to highlight their technique. The first video shows an attacker hundreds of yards away sending infrared signals to a camera. The second video shows the camera infected with malware responding to covert signals by exfiltration data, including passwords and selected passages of the book The Adventures of Tom Sawyer.

According to Dr. Guri, "Security cameras are unique in that they have 'one leg' inside the organization, connected to the internal networks for security purposes, and 'the other leg' outside the organisation, aimed specifically at a nearby public space, providing very convenient optical access from various directions and angles."

Attackers can also use this novel covert channel to communicate with malware inside the organisation. An

continue on page 76

ROBO-COPS AROUND THE WORLD

Police Robots are Taking Over the World!!!

Cleveland, Ohio, USA

PD's Griffin has been enlisted by the Cleveland Police Department to safeguard locals. Built by students from the local community college and standing only 12 inches tall, the six-wheeled rover is designed to go places police can't fit, like under a car or behind dumpsters to look for explosives. Griffin is also equipped with a camera and light which allows police to scope out the situation from a monitor at a safe distance.

Unlike larger bomb squad and military grade robots, like the one police strapped an explosive to in Dallas, Griffin is light enough to be deployed quickly without needing to be hauled out in a big truck and just one of the 40 robots that Ohio police have on hand.

Kinshasa, Congo

In the bustling capital city of the Democratic Republic of Congo, according to reports in The Guardian, city officials have installed several giant solar-powered robot traffic cops in 2013 in an effort to reduce deaths and get more people to follow traffic rules. Looking dapper in cool sunglasses, the massive humanoid robots stand at busy intersections as kind of an all-in-one traffic light/crosswalk/traffic camera.

The robots direct traffic with arms that signal red and green flags as well as usher pedestrians safely across wide, busy roads. The humanoids were designed by Women's Technology, an association of female and male engineers in Congo and like every police robot on this list, are equipped with surveillance cameras that send footage back to police in an effort to deter dangerous driving.

Israel

A 26-pound, eleven 11-inch-tall robot is packing a 9mm Glock pistol is the Israeli Police Force's latest member. Designed by Israeli firm General Robotics Ltd and assisted by the Israeli Police Counter Terrorism Unit, the Dogo can fire up to five rounds in two seconds. This small land rover can enter a house quietly, climb stairs, and even maneuver over obstacles. Equipped with eight cameras and two-way audio, the Dogo allows police to communicate with and fire upon suspects without risking their lives. If law enforcement are not looking to kill, the Dogo can also carry pepper spray or a dazzling light module to cause temporary blindness.

Lesvos, Greece

The coast guard in Lesvos, Greece recently started deploying robotic life-preservers to rescue Syrian refugees travelling across the Mediterranean Sea. Refugee's boats are often underpowered, overloaded and lack sufficient life jackets. Everyday authorities scramble to save people from boats that have capsized, run out of fuel, or wrecked in the rough waters. The robot helping them is named Emily which is an acronym for Emergency Integrated Lifesaving Lanyard and is a project by researchers at Texas A&M University. Emily is a floatation device that zooms across the water at 20 miles per hour tethered to a 2,000 ft. rope attached to a rescue ship. Emily makes fetching people who are not drowning faster which leaves the human rescue team free time to rescue victims who require urgent assistance.

Pohang, South Korea

Correctional officers at Pohang prison in South Korea have enlisted the help of robots to assist in keeping watch for them. At 5-feet tall, the Robo-Guard is equipped with 3D cameras and software to recognise inmate behavior. The robot's makers say it is able to report when something seems abnormal, such as fights or an inmate on the floor. The human in the control center can also communicate with prisoners via the robot's two-way radios. It is however unclear if the robots were put into full-time use in South Korea after the tests in 2012, though reports indicate that South Korea is currently building robo-guards to keep patrol during the 2018 Winter Olympics in Pyeongchang.

Los Angeles, California, USA

The Bat Cat which is short for Bomb Assault Tactical Control Assessment Tool is the Los Angeles Police Department's radio-controlled monster. Designed to pick up a car bomb with its 50-foot telescoping arm, the unmanned ground vehicle reaches top speed at six miles per hour. While it was originally designed to remove massive explosives, the Bat Cat can also rip through a house in minutes, according to The Los Angeles Times,which reported that the LAPD used it to tear down the walls of a home during a standoff in 2011. Cops can switch out the end of the telescoping arm with a claw, a bucket, a forklift, or battering rams, and it can handle a payload of around 12,000 pounds, more than enough to haul your typical car bomb far from harm's way. The Bat Cat was constructed on the chassis of a Caterpillar Telehandler.

Japan

Just like in an action movie, the Japanese police are using drones to take down drones, without shooting at them which would cause debris. Instead police are using a net. Japanese police introduced a net-wielding drone fleet earlier this year to catch suspicious looking small unmanned aircrafts that fly over sensitive government locations like butterflies. It takes a giant net to catch a drone and the police fleet is equipped with a 6.5-foot-by-10-foot lattice.

In 2016 the BBC reported that police deployed the net drones in response to a drone carrying a non-harmful amount of radioactive sand that landed on the roof of the Prime Minister Shinzo Abe's house, a stunt that turned out to be a protest by an anti-nuclear activist. Japan's drone-catching drone certainly seems a lot safer than the Dutch National Police Force's solution whereby eagles were trained to take down unauthorised drones.

Uttar Pradesh, India

Riot-Control Skunk Drones were purchased last year by the police in India's Uttar Pradesh region. Built to shower crowds with pepper spray and paintballs, the drone, manufactured by South African firm Desert Wolf, can hover mid-air over a protest and fire up to 20 paintballs (or other "non-lethal" ammunition) per second while simultaneously dispersing tear gas pellets onto people.

Police control the drone from the ground, which levitates via eight motors that each power a 16-inch propeller. The robots are also outfitted with onboard speakers so authorities can communicate with crowds, as well as bright strobe lights and "eye safe" lasers to disorient and disperse a gathering and of course, no drone is complete without surveillance capability. The Skunk features a thermal camera, a HD camera and an onboard microphone for post review.

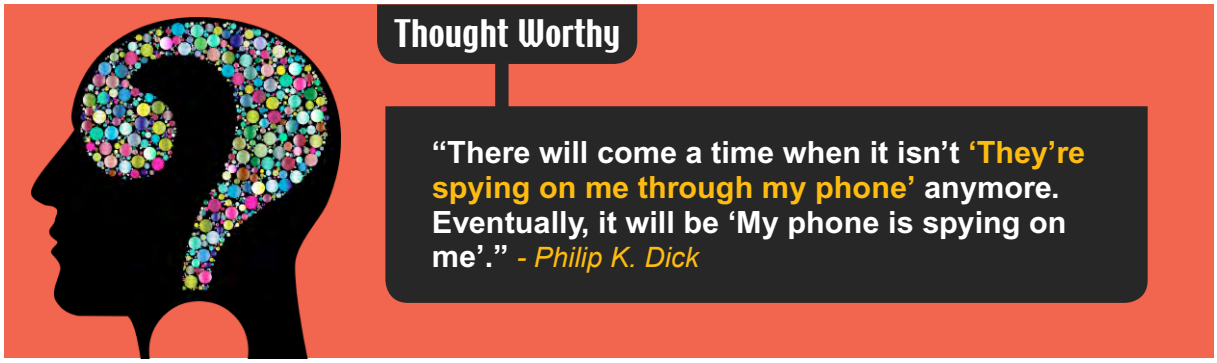
> "To transmit sensitive information, the attacker uses the camera's IR-emitting LEDs, which are typically used for night vision. The researchers showed how malware can control the intensity of the IR to communicate with a remote attacker that can receive signals with a simple camera without detection. Then the attacker can record and decode these signals to leak sensitive information."

attacker can infiltrate data, transmitting hidden signals via the camera's IR LEDs. Binary data such as command and control (C&C) messages can be hidden in the video stream, recorded by the surveillance cameras, and intercepted and decoded by the malware residing in the network.

"Theoretically, you can send an infrared command to tell a high-security system to simply unlock the gate or front door to your house," Guri says.

The research team also includes Dr. Dima Biekowski, Shamoon College of Engineering, and Prof. Yuval Elovici, director of the Cyber Security Research Center, a member of BGUs Department of Software and Information Systems Engineering and director of Deutsche Telekom Innovation Labs @ BGU.

For more information, please visit www.aabgu.org SST



First Half 2017 Breach Level Index Report: Identity Theft and Poor Internal Security Practices Take a Toll

Singapore – Gemalto, the world leader in digital security, today released the latest findings of the Breach Level Index, a global database of public data breaches, revealing 918 data breaches led to 1.9 billion data records being compromised worldwide in the first half of 2017. Compared to the last six months of 2016, the number of lost, stolen or compromised records increased by a staggering 164%. A large portion came from the 22 largest data breaches, each involving more than one million compromised records. Of the 918 data breaches more than 500 (59% of all breaches) had an unknown or unaccounted number of compromised data records.

The Breach Level Index is a global database that tracks data breaches and measures their severity based on multiple dimensions, including the number of records compromised, the type of data, the source of the breach, how the data was used, and whether or not the data was encrypted. By assigning a severity score to each breach, the Breach Level Index provides a comparative list of breaches, distinguishing data breaches that are not serious versus those that are truly impactful.

According to the Breach Level Index, more than 9 billion data records have been exposed since 2013 when the index began benchmarking publicly disclosed data breaches. During the first six months of 2017, more than ten million records were compromised or exposed every day, or one hundred and twenty-two records every second, including medical, credit card and/or financial data or personally identifiable information. This is particularly concerning, since less than 1% of the stolen, lost or compromised data used encryption to render the information useless, a 4% drop compared to the last six months of 2016.

"IT consultant CGI and Oxford Economics recently issued a study, using data from the Breach Level Index and found that two-thirds of firms breached had their share price negatively impacted. Out of the 65 companies evaluated the breach cost shareholders over $52.40 billion," said Jason Hart, Vice President and Chief Technology Officer for Data Protection at Gemalto. "We can expect that number to grow significantly, especially as government regulations in the U.S., Europe and elsewhere enact laws to protect the privacy and data of their constituents by associating a monetary value to improperly securing data. Security is no longer a reactive measure but an expectation from companies and consumers."

Primary Sources of Data Breaches

Malicious outsiders made up the largest percentage of

continue on page 80

"Most of the industries the Breach Level Index tracks had more than a 100% increase in the number of compromised, stolen or lost records. Education witnessed one of the largest increases in breaches up by 103% with an increase of over 4,000% in the number of records. This is the result of a malicious insider attack compromising millions of records from one of China's largest comprehensive private educational companies."

data breaches (74%), an increase of 23%. However, this source accounted for only 13% of all stolen, compromised or lost records. While malicious insider attacks only made up 8% of all breaches, the amount of records compromised was 20 million up from 500,000 an increase of over 4,114% from the previous six months.

Leading Types of Data Breaches

For the first six months of 2017, identity theft was the leading type of data breach in terms of incident, accounting for 74% of all data breaches, up 49% from the previous semester. The number of records compromised in identity theft breaches increased by 255%. The most significant shift was the nuisance category of data breaches representing 81% of all lost, stolen or compromised records. However, in terms of the number of incidents, nuisance type attacks were only slightly over 1% of all data breaches. The number of compromised records from account access attacks declined by 46%, after a significant spike in the 2016 BLI full year report.

Biggest Industries Affected by Data Breaches

Most of the industries the Breach Level Index tracks had more than a 100% increase in the number of compromised, stolen or lost records. Education witnessed one of the largest increases in breaches up by 103% with an increase of over 4,000% in the number of records. This is the result of a malicious insider attack compromising millions of records from one of China's largest comprehensive private educational companies. Healthcare had a relatively similar amount of breaches compared to the last six months of 2016, but stolen, lost or compromised records increased 423%. The U.K's National Health Service was one of the top five breaches in the first half with over 26 million compromised records. Financial services, government and entertainment were also industries that experienced a significant jump in the number of breached records, with entertainment breach incidents increasing 220% in the first six months of 2017.

Geographic Distribution of Data Breaches

North America still makes up the majority of all breaches and the number of compromised records, both above 86%. The number of breaches in North America increased by 23% with the number of records compromised skyrocketing by 201%. Traditionally, North America has always had the largest number of publicly disclosed breaches and associated record numbers, although this is poised to change in 2018 when global data privacy regulations like the European General Data Protection Regulation (GDPR) and Australia's Privacy Amendment (Notifiable Data Breaches) Act are enforced. Europe currently only had 49 reported data breaches (5% of all breaches), which is a 35% decline from the previous six months. SST

BT and KPMG Warn Businesses Against Cyber Security Traps

Investing in IT security products alone is no silver bullet in battle against cyber crime

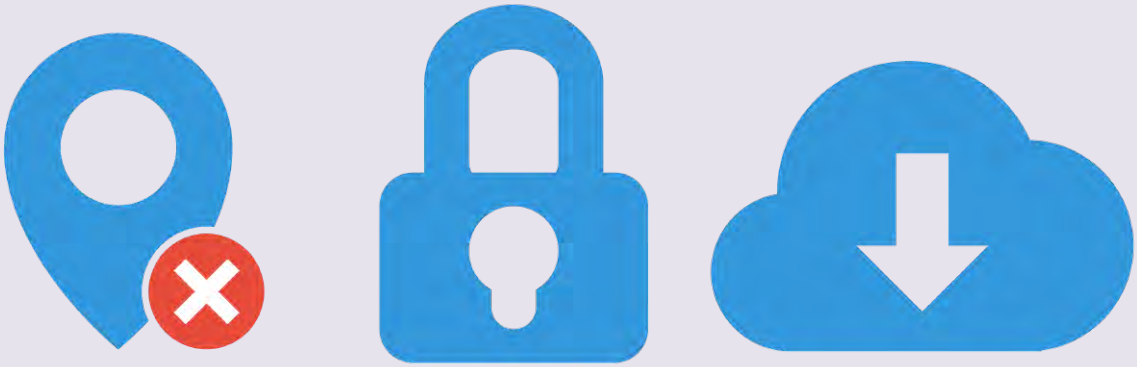
In the wake of high-profile global ransomware attacks such as WannaCry and Petya, BT and KPMG have released a new cyber security report offering practical advice to businesses of all sizes on how best to manage their security journey and turn it into a business opportunity.

The new report, "The cyber security journey – from denial to opportunity", warns businesses against falling into dangerous traps as they deal with the complexity of securing a digital enterprise. These include being stuck in 'Denial' and 'Worry' phases at one end of the spectrum, and 'False Confidence' and 'Hard Lessons' at the other end.

While the report stresses that investment in technology such as firewalls and antivirus protection is essential 'good housekeeping' practice at the start of the security journey, firms should avoid throwing money away on IT security products as a knee-jerk reaction. This is especially true for companies who have matured from the stage of 'denial' into the stage of constant 'worry', where investing in the latest technology can be viewed as the silver bullet to the problem. This common mistake can make firms a target, not just for cyber criminals, but also for over-zealous IT salespeople.

Businesses must first assess their current controls against industry best practices, such as guidance and available resources offered by the Cyber Security Agency of Singapore, to identify any gaps and prioritise essential areas in which to address. Furthermore, everyone in the organisation, from the board down, must take responsibility for maintaining high standards of cyber hygiene, while businesses must invest in training and raise awareness amongst staff. This can help turn employees from the weakest point in any security chain into every company's greatest asset in the fight to protect data.

Mark Hughes, CEO, BT Security, said: "The global scale of the recent ransomware attacks showed the astonishing speed at which even the most unsophisticated of attacks can spread around the world. Many organisations



continue on page 82

could have avoided these attacks by maintaining better standards of cyber hygiene and getting the basics right. These global incidents remind us that every business today - from the smallest sole trader through to SMEs and large multinational corporations - needs to get to grips with managing the security of their IT estate, as well as their people and processes. This report aims to help secure the digital enterprise by navigating businesses through their cyber security journey."

David Ferbrache, Technical Director in KPMG's cyber security practice, said: "The recent spate of cyber-attacks is keeping cyber risk at the top of the business agenda, and as such investments are being made. The business community needs to avoid knee-jerk reactions as cyber security is a journey – not a one size fits all issue, and getting the basics like patching and back-ups right matters. It's important to build a security culture, raise awareness amongst staff, and remember that security needs to enable business, not prevent it.

"In order to address these risks and gain true leadership in cyber security, the report calls on firms to focus on good governance processes, the proper integration of technologies and to consider outsourcing some less critical aspects of their security to a trusted partner."

"Cyber threats are evolving and businesses face ruthless criminal entrepreneurs. The solution isn't jargon ridden technology silver bullets but one that involves a community effort in a world where business boundaries are vanishing. With criminals getting increasingly creative about finding the weakest link, the CISOs of the future need to care about digital risk, help the business seize opportunities and build cyber resilience."

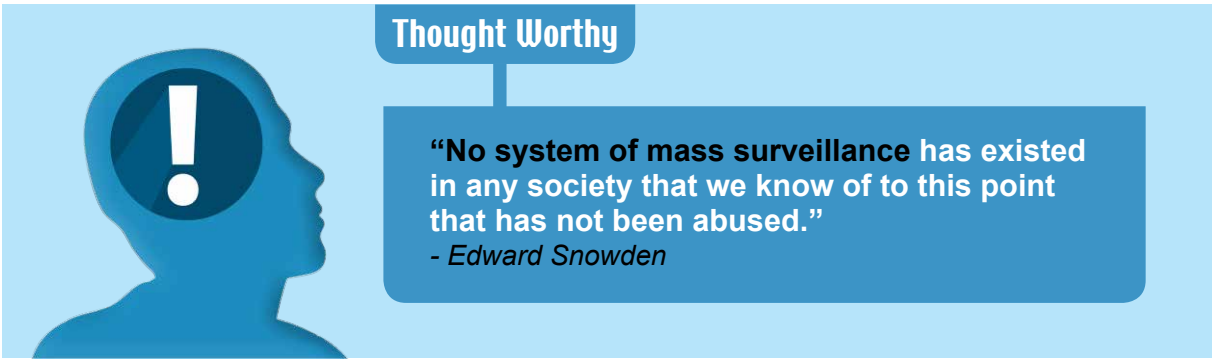
Although cyber security issues are increasingly discussed at board level today, the report claims that those discussions are too infrequent and are treated as a separate and disconnected issue from broader operational risk. All too often, the issue of cyber security is not incorporated into the overarching business strategy.

The report also argues that overly complex IT architecture can worsen security gaps. This is especially the case if the technology deployed is too difficult to use or there is a lack of integration.

In order to address these risks and gain true leadership in cyber security, the report calls on firms to focus on good governance processes, the proper integration of technologies and to consider outsourcing some less critical aspects of their security to a trusted partner. This, combined with the sharing of intelligence, good practice and hard-won lessons among a network of peers and beyond would put the company in a position to think about cyber security differently. Namely, not as a risk which is discussed by the board perhaps twice a year, but as a business opportunity and enabler for digital transformation.

The report comes at a time especially relevant to Singapore as the country embarks on a holistic, national cyber security strategy to ensure industries, businesses and the nation embrace digitalisation and transformation in a safe, secure environment.

For more information, please visit: www.globalservices.bt.com SST



Cyber Crime Drains $11.7 Million Per Business Annually, Up 62 Percent in Five Years

Malware infections globally are the most expensive cyber attacks – costing $2.4 million per incident

Costly cyber attacks are having a significant and growing financial impact on businesses worldwide. According to new research published today by Accenture and the Ponemon Institute, in 2017 the average cost of cyber crime globally climbed to $11.7 million per organisation, a 23 percent increase from $9.5 million reported in 2016, and represents a staggering 62 percent increase in the last five years. In comparison, companies in the United States incurred the highest total average cost at $21.22 million while Germany experienced the most significant increase in total cyber crime costs from $7.84 million to $11.15 million. This surge follows a recent string of infamous malware attacks including WannaCry and Petya, which cost several global firms hundreds of millions of dollars in lost revenues.

The "Cost of Cyber Crime Study" surveyed 2,182 security and IT professionals in 254 organisations worldwide and found that the number of cyber attacks has shown no sign of slowing down since the Ponemon Institute began the research in 2009. Key findings of the study include the following:

- On average, a company suffers 130 breaches per year, a 27.4 percent increase over 2016 and almost double what it was five years ago. Breaches are defined as core network or enterprise system infiltrations.

- Companies in the financial services and energy sectors are the worst hit, with an average annual cost of $18.28 million and $17.20 million respectively.

- The time to resolve issues is showing similar increases. Among the most time-consuming incidents are those involving malicious insiders, which take on average 50 days to mitigate while ransomware takes an average of more than 23 days.

- Malware and Web-based attacks are the two most costly attack types with companies spending an average of $2.4 million and $2 million respectively.

"The costly and devastating consequences businesses are suffering, as a result of cyber crime, highlights the

"Companies in the United States incurred the highest total average cost at $21.22 million while Germany experienced the most significant increase in total cyber crime costs from $7.84 million to $11.15 million. This surge follows a recent string of infamous malware attacks including WannaCry and Petya, which cost several global firms hundreds of millions of dollars in lost revenues."

continue on page 84

growing importance of strategically planning and closely monitoring security investments. As this research shows, making wise investments in innovation can certainly help make a significant difference when cyber criminals strike," said Kelly Bissell, managing director of Accenture Security. "Keeping pace with these more sophisticated and highly motivated attacks demands that organisations adopt a dynamic, nimble security strategy that builds resilience from the inside out – versus only focusing on the perimeter with an industry-specific approach that protects the entire value chain, end-to-end."

Security Technology Spending Out of Balance

Of the nine security technologies evaluated, the highest percentage spend was on advanced perimeter controls, yet companies deploying these security solutions only realised an operational cost savings of $1 million associated with identifying and remediating cyber attacks, suggesting possible inefficiencies in the allocation of resources. Among the most effective categories in reducing losses from cyber crime are security intelligence systems, defined as tools that ingest intelligence from various sources that help companies identify and prioritise internal and external threats. They delivered substantial cost savings of $2.8 million, higher than all other technology types included in this study. Automation, orchestration and machine learning technologies were only deployed by 28 percent of organisations – the lowest of the technologies surveyed – yet provided the third highest cost savings for security technologies overall at $2.2 million.

Financial Consequences of Cyber Attacks Are Surging

Researchers considered four main impacts on organisations that suffered a cyber attack: business disruption, loss of information, loss of revenue and damage to equipment. The most damaging of those today is loss of information, mentioned by 43 percent of organisations represented in the study. In contrast, the cost of business disruption, such as business process failures following an attack, has decreased from 39 percent in 2015 to 33 percent in this year's research.
"The foundation of a strong and effective security program is to identify and 'harden' the most-high value assets," said Dr. Larry Ponemon, chairman and founder of the Ponemon Institute. "While steady progress has been made in improving cyber defense, a better understanding of the cost of cyber crime could help businesses bridge the gap between their own vulnerabilities and the escalating creativity and numbers of threat actors."

Costs Per Organisation Vary Widely By Country and Type of Cyber Attack

Australia reports the lowest total average cost from a cyber attack at $5.41 million, while the United Kingdom had the lowest change over the last year from $7.21 million to $8.74 million. Japan experienced a 22 percent increase in costs to $10.45 million – the third highest increase of the countries in the survey.

"Costs also vary considerably by the type of cyber attack. U.S. companies are spending more to resolve all types of cyber attacks, especially for malware and Web-based attacks ($3.82 million and $3.40 million per incident, respectively)."

Costs also vary considerably by the type of cyber attack. U.S. companies are spending more to resolve all types of cyber attacks, especially for malware and Web-based attacks ($3.82 million and $3.40 million per incident, respectively). For companies in Germany and Australia, 23 percent of total annual cyber incident costs are due to malware attacks. In France, 20 percent of the total cyber crime annual costs are attributed to Web-based attacks. Denial of service attacks account for 15 percent of total cyber crime annual costs in both Germany and the United Kingdom.

Steps to Improve Effectiveness of Cybersecurity Efforts

By taking the following three steps, organisations can further improve the effectiveness of their cybersecurity efforts to fend off and reduce the impact of cyber crime:

- Build cybersecurity on a strong foundation: invest in the 'brilliant basics' such as security intelligence and advanced access management and yet recognise the need to innovate to stay ahead of hackers.
- Undertake extreme pressure testing: Organisations should not rely on compliance alone to enhance their security profile but undertake extreme pressure testing to identify vulnerabilities more rigorously than even the most highly motivated attacker.
- Invest in breakthrough innovation: Balance spend on new technologies, specifically analytics and artificial intelligence to enhance program effectiveness and scale value.

For more information please visit: www.accenture.com SST

Singapore signs Memorandum of Cooperation on Cybersecurity with Japan at the Sidelines of SICW 2017

Singapore and Japan signed a Memorandum of Cooperation (MOC) to strengthen cybersecurity cooperation between the two countries on 18 September 2017.

The MOC was signed by Mr David Koh, Chief Executive, Cyber Security Agency of Singapore (CSA), and Dr Ikuo Misumi, Deputy Director-General of the National Center of Incident Readiness and Strategy for Cybersecurity (NISC), Japan. The signing ceremony took place at The St. Regis Singapore Hotel.

The MOC covers cybersecurity cooperation in key areas including regular policy dialogues, information exchanges, collaborations to enhance cybersecurity awareness, joint regional capacity building efforts, as well as sharing of best practices between both countries.

continue on page 86

Mr Koh said, "Singapore and Japan have been working closely together on various cybersecurity initiatives at both the bilateral and multilateral levels. This MOC will serve to bring our cooperation and relations a step further. I am confident that we will continue to have fruitful exchanges and move forward to operationalise our cybersecurity priorities."

Prior to the signing of this MOC with Japan, CSA had previously signed six Memoranda of Understanding with Australia, France, India, the Netherlands, the United Kingdom, the United States, and a Joint Declaration on cybersecurity cooperation with Germany.

"Singapore and Japan have been working closely together on various cybersecurity initiatives at both the bilateral and multilateral levels. This MOC will serve to bring our cooperation and relations a step further. I am confident that we will continue to have fruitful exchanges and move forward to operationalise our cybersecurity priorities."

- Mr David Koh, Chief Executive of Cyber Security Agency of Singapore (CSA)

About Cyber Security Agency of Singapore

The Cyber Security Agency of Singapore (CSA) provides dedicated and centralised oversight of national cyber security functions, and works with sector leads to protect Singapore's critical services. It also engages with various industries, and stakeholders to heighten cyber security awareness as well as to ensure the holistic development of Singapore's cyber security landscape. The Agency is part of the Prime Minister's Office and is managed by the Ministry of Communications and Information.

For more information, please visit: www.csa.gov.sg SST

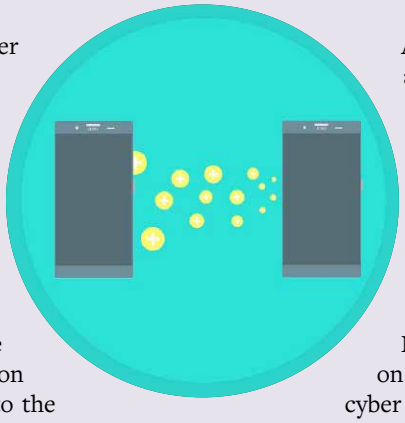
Darktrace Commentary in Response to Singapore's National Day Rally

By Sanjay Aurora, Managing Director, Asia-Pacific at Darktrace

During this year's National Day Rally, Prime Minister Lee Hsien Loong addressed Singapore's Smart Nation vision and how we need to accelerate our use of IT to create opportunities and make Singapore an "outstanding place to live, work and play." This includes the mainstream adoption of electronic payments, deployment of sensor networks and using big data.

While we should be excited at the prospect of new possibilities, these technologies bring a new type of cyber risk into the equation. Local organisations will therefore need to relook their fundamental approach to cyber defence as a part of realising their Smart Nation ambitions.

continue on page 87



Cashless payments no doubt deliver convenience, ease of transaction and allow individuals to better keep track of spending. At the same time, we've seen a rise in text message scams called "smishing," which can infect smartphones and result in the theft of personal information.

Sensor networks or IoT, combined with big data, can help Singapore understand everything from carbon monoxide emissions and traffic flow to the number of people using the crosswalks. It has the potential to make our environment and everyday lives more efficient and sustainable. However, unsecured IoT devices, from smart lamp posts and sensors to network-connected biometric sensors and even fish tanks, can provide additional entry points for cyber-criminals.

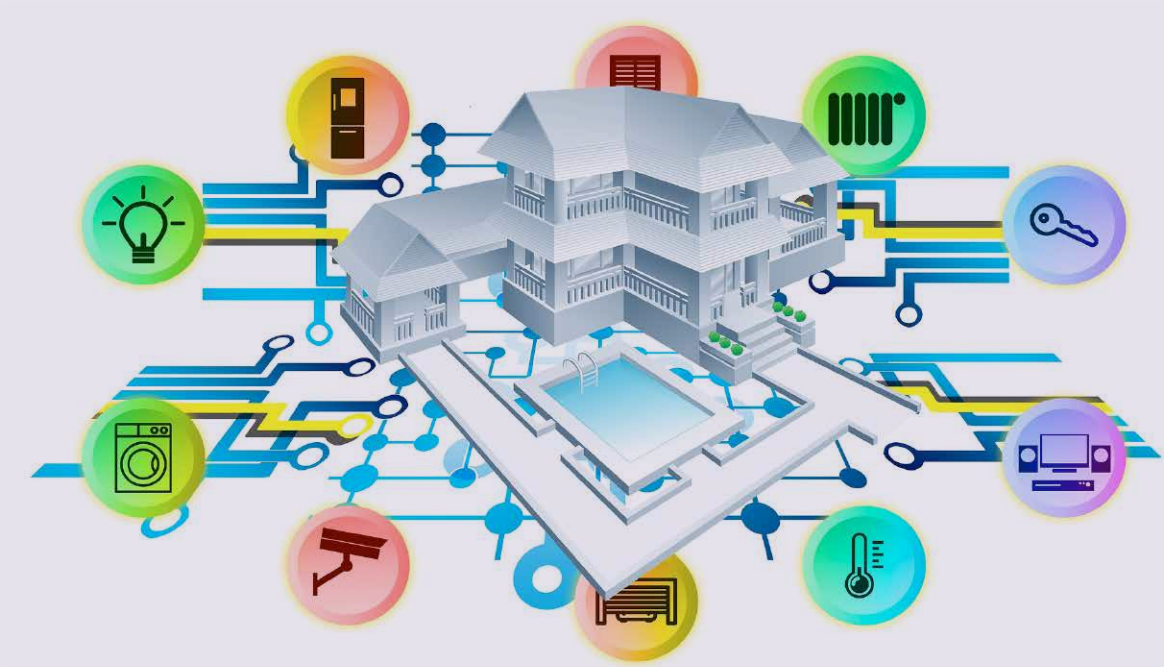
"Sensor networks or IoT, combined with big data, can help Singapore understand everything from carbon monoxide emissions and traffic flow to the number of people using the crosswalks. It has the potential to make our environment and everyday lives more efficient and sustainable."

As we've seen with recent cyber-attacks, today's cyber-criminals are no longer purely after financial gain. They endeavour to sow disruption and erode public trust in an organisation's ability to safeguard data and keep our everyday lives running normally.

The success of Singapore's Smart Nation vision will be heavily dependent on its ability to mitigate new forms of cyber risk. Alongside speed in the delivery of public services, business transactions and even social interactions, there is a pressing need for speed in addressing cyber-threats that can come from anywhere and move faster than ever before.

These threats are outpacing the efforts of human security teams and organisations can no longer hide behind a cloak of ignorance or a lack of resources. There is a solution – governments around the world, including Singapore's, are starting to focus their attention on AI and this new class of technology can be used in cyber defence to autonomously detect and halt novel attacks. In fact, this is already being adopted by local companies big and small.

For the first time, local organisations have the opportunity to be on the front foot. Cyber security does not need to be seen as a necessary evil or a set of limiting technologies, policies and procedures that cripple business growth. Rather, it becomes an enabler that would be imperative for Singapore's Smart Nation transition. SST



IoT and Security - What the Internet of Things Means to Security

Increased Connectivity Can Potentially Mean an Increased Risk of Attack

In 2013, there were approximately 9.9 million objects and/or devices connected to the Internet of Things (IoT), and by the year 2020, that figure is expected to jump astronomically. According to the Spark Labs Global Ventures' Internet of Things & Hardware Industry Report 2016, Verizon predicts that the number of B2B IoT connections will increase to 5.4 billion by 2020. According to Gartner, the overall number is predicted to be 20.8 billion by 2020. Virtually all the devices which we use around the home and in the work place to make life easier will be connected to the Internet, which will present some amazing opportunities for innovation and enhanced usability. On the other hand, it will also provide a plethora of targets for hacking by the criminal-minded, and open up a whole new area of risk for security systems.

There are a number of threats which will come into play with the coming increased connectivity of the IoT, including the theft of confidential or private data, unauthorised controlling of devices, and the denial of service to applications associated with the devices. While the security threats to household items are of great concern, just imagine the potential for a cyber attacker to take control of Supervisory Control and Data Acquisition Systems (SCADA) or an Industrial Control System (ICS)!

Security Challenges Presented by the IoT

Some of the challenges presented by ubiquitous connection to the IoT are the same existing challenges for infrastructures administered on a large scale:

- **Authentication:** Users, devices, and applications must all be authenticated as legitimate and authorised for access.
- **Auditing:** An accurate log must be in place to track all activity, so threats can be identified.
- **Administration:** Security practices must be in place throughout all points of the network.
- **Encryption/decryption:** Critical data needs to be encrypted against interception by unauthorized individuals.
- **Data integrity:** Critical systems must be protected against corruption or hijacking by cyber attackers.

On the other hand, there are also some brand new issues posed by global connectivity to the IoT:

- **Wider range of device types:** In the coming years, almost every conceivable kind of device could be connected to the IoT, which means that some kind of security scheme must be devised for its protection. Since every single device provides a security surface which can be exploited by criminals, it must be factored into the overall security scheme.
- **Less controlled environment:** Security measures are not the same all around the globe, but devices connected to the IoT will be global in their

continue on page 89

"While the security threats to household items are of great concern, just imagine the potential for a cyber attacker to take control of Supervisory Control and Data Acquisition Systems (SCADA) or an Industrial Control System (ICS)!"

establishment. This creates the potential for exploitation at the weaker security points, and because of universal connectivity, any exploited weak point has the potential to affect almost everyone.

- **More attack points:** The sheer number of devices online will require a staggering level of commitment to security, because each of those devices will represent a potential attack point for criminal-minded individuals.

MSSP to Manage All Security Threats

All these issues can be managed by a forward-thinking managed security services provider (MSSP), using available security data and a comprehensive program of analytics. A highly reputable and effective provider like GlassHouse Systems is on the alert for every new security threat. They aim to deliver the best protection for all your potentially vulnerable security surfaces.

For more information, please visit: www.ghsystems.com SST

Huawei Launches the First All-Cloud, Network-wide Smart Video Cloud Solution

Driving the Evolution of Videos to Enable Actionable Intelligence that Improves City Safety

At Huawei Connect 2017, Huawei launched the industry's first all-cloud, network-wide smart video cloud solution, together with industry partners including Yitu, SenseTime, NetPosa, Harzone, MIMOS, and Qognify. The open cloud platform benefits from a vast ecosystem of partners delivering a wide-range of smart video

continue on page 90

analytic algorithms. This provides a strong computing engine that supports public safety video application services and accelerates video application innovation to help public safety organisations better serve and protect citizens.

As cities embrace digital transformation, video is becoming an important tool for public safety management and city governance. In China, over 60% of public safety cases are solved using video. However, social video systems and security video systems typically operate independently, which makes video and data sharing difficult. Cross-regional crimes are increasing and without a collaborative solution, obtaining and analysing video feeds consumes a significant amount of time, manpower, and costs. There is a pressing need among public safety agencies to find more efficient and open video application capabilities to address these challenges.

Huawei's Smart Video Cloud constructs "One City, One Cloud" concept

Kevin Bai (the fifth from left), General Manager of Government Solutions Department, Huawei Enterprise Business Group, and partners launched the Smart Video Cloud Solution.

Kevin Bai, General Manager of Government Solutions Department, Huawei Enterprise Business Group, said: "Huawei's Smart Video Cloud is based on an open cloud platform, which supports algorithms and applications from many partners to enable effective video sharing. Network-wide distributed smart analysis significantly increases video analysis efficiency; and in cross-departmental and cross-regional cases, the solution can rapidly respond with analysis results. In addition, converged Big Data technologies can uncover hidden insights from videos to support the work of public safety agencies. The video cloud can also be used as a service for other organisations or institutions, for example to support traffic regulation, detect the crowd flow at scenic spots, locate missing people, and many other public services. This solution allows videos to play a disruptive role in public safety applications, evolving from purely surveillance to generating actionable intelligence which takes city safety to a new level."

In the past few years, China has experienced a breakthrough in video networking development, and thus promoting the construction of the video application ecosystem. Discussing Shenzhen's public safety management experience, Zhang Yong, Captain of Shenzhen's Public Security Bureau Video Surveillance Police Detachment, said: "Videos have played a key role in improving security for Shenzhen's citizens. We have worked with Huawei for the past two years to develop a comprehensive video platform, which has helped us solve countless cases. Huawei's video cloud, which combines centralised computing and edge computing capabilities, will help us further enhance our video application services to ensure peace in Shenzhen's communities."

Huawei Displays A Variety of the Latest C-C4ISR Collaborative Public Safety Solutions

At Huawei Connect 2017, under the theme of "New ICT, the Road to Collaborative Public Safety", Huawei displayed the latest C-C4ISR collaborative public safety solutions. Among them, many new solutions and applications were

continue on page 91

showcased for the first time:

- The Huawei Video Cloud Platform brought together 16 partners to demonstrate how a large-scale video application ecosystem enables a city council to distribute different tasks to different branch offices to perform video networking and smart analysis for dangerous object identification, crowd analysis, facial recognition at a far distance, and many other tasks. The demonstration showed how the platform strengthens the video application services of public safety customers.

- Applications from Vastio, Xinyi, MiningLamp, Zenith and other partners running on Huawei's Big Data platform create an information command and action-infused smart command center. Various usage scenarios were displayed, such as how to use Big Data and machine learning to predict risks, gain insight into the opinions in public media, and prevent and alleviate traffic congestion.

- An End-to-end digitised emergency response management solution helps public safety agencies efficiently manage natural or man-made emergencies and protect citizens.

- An all-in-one station with the industry's highest level of integration increases deployment efficiency by 56%, and can achieve ubiquitous alarms, investigation, and monitoring coverage.

- iOMC, a one-stop full-lifecycle service platform with unified operations and maintenance (O&M) capabilities for safe cities, integrates the domain of every product, and performs unified monitoring and unified alarm dispatching based on the service scenario.

"Huawei has taken the lead to introduce a public safety industry enablement platform at HUAWEI CONNECT 2017. The platform serves as a smart warehouse market where capabilities commonly used in the public safety industry, including a wide-range of video smart analysis capabilities in video cloud, integrated communications capabilities, IoT, and Big Data, are readily available for delivery."

Hong-Eng Koh, Global Chief Public Safety Expert for Huawei Enterprise Business Group, explained collaborative public safety.

The digital transformation of the public safety industry will depend on the maturity of the applications market, and there will be greater demand for collaboration between these applications. For this reason, Huawei has taken the lead to introduce a public safety industry enablement platform at HUAWEI CONNECT 2017. The platform serves as a smart warehouse market where capabilities commonly used in the public safety industry, including a wide-range of video smart analysis capabilities in video cloud, integrated communications capabilities, IoT, and Big Data, are readily available for delivery. The user or software provider can use a "building-block" approach to select their required capability components, making it easy to develop new service applications quickly. The solution can empower the entire ecosystem and drive momentum in the journey to collaborative public safety, presenting new opportunities for ecosystem development to help partners achieve business success while growing with Huawei.

To date, 197 of the Fortune Global 500 companies and 45 of the top 100 enterprises have chosen Huawei as their partner for digital transformation. These companies are realising the benefits of Huawei's one-stop, innovative ICT infrastructure platform with cloud-pipe-device integration and open ecosystem for customers across various industries.

For more information, please visit www.huawei.com SST

IBM and VMware Partnership Speeds Cloud Adoption in the Enterprise

More than 1,400 Enterprises such as Honeywell International Tapping into IBM Cloud for VMware Solutions

Singapore – At VMworld® Europe 2017, IBM and VMware, Inc. announced that more than 1,400 enterprises in nearly every industry around the world are extending their VMware environments to the IBM Cloud. Through the partnership, clients such as Honeywell International and Vodafone are using IBM Cloud's global reach and cloud-native services, and the infrastructure and operational consistency of VMware Cloud Infrastructure, to create new business opportunities.

IBM and VMware announced new solutions to further the partnership and IBM is launching network control and visibility solutions from F5 Networks and Fortinet so that enterprises can continue to extend their VMware environments, as they are, to the public cloud.

In 2016, IBM and VMware set out to tackle a pressing industry challenge: extending existing VMware workloads from on-premises environments to the cloud without having to retool operations, re-architect applications and re-design security policies. Enterprises are able to run their VMware workloads in the cloud and leverage IBM's AI and analytics services as an extension of their VMware deployment. IBM Cloud for VMware solutions are available across IBM's global network of nearly 60 cloud data centers in 19 countries.

IBM and VMware Partnership Fuels Global Enterprise Adoption

Client adoption continues to grow as enterprises such as the Performance Materials and Technology (PMT) Division of Honeywell International adopt these solutions. Honeywell, a global leader in designing and creating software-based systems to safely and efficiently operate complex industrial facilities, selected IBM Cloud as the foundation for its Open Virtual Engineering

> "Honeywell, a global leader in designing and creating software-based systems to safely and efficiently operate complex industrial facilities, selected IBM Cloud as the foundation for its Open Virtual Engineering Platform (VEP), which enables users to build and test engineering processes in a highly reliable and security-rich cloud-based environment."

continue on page 93

Platform (VEP), which enables users to build and test engineering processes in a highly reliable and security-rich cloud-based environment.

By moving to the IBM Cloud, Honeywell seamlessly transitioned its VMware-based environment and is able to take advantage of existing tools, technologies and operational processes in the cloud. Honeywell is also able to leverage advanced data protection and security capabilities from HyTrust and Intel, both critical factors in the company's decision to use IBM Cloud.

"Honeywell is developing the technologies of tomorrow so that manufacturing and plant operators can better address challenges such as efficiency, productivity, reliability, safety, and security," said Vimal Kapur, president, Honeywell Process Solutions. "The partnership between IBM and VMware is enabling Honeywell to deliver new industrial automation technologies like the Open Virtual Engineering Platform for our customers around the world. The global reach of the IBM Cloud, the operational consistency of VMware across on-premises and cloud environments and the ability to leverage HyTrust and Intel technology for additional security were important to us."

> "IBM's partnership with VMware has enabled more than 1,400 enterprises to quickly and easily transition to the cloud to securely scale and enhance their workloads with full access to a rich catalog of IBM Cloud services, including AI, data and analytics, IoT, serverless and more."

Additionally, through a new agreement with IBM, Vodafone announced today that it is offering an international service that enables enterprises to support the movement of VMware-based workloads on a Vodafone Hosted Private Cloud to and from the IBM Cloud.

To extend the reach of IBM Cloud for VMware solutions, IBM and Dell EMC today announced an agreement to help accelerate cloud adoption by providing Dell EMC's commercial customers access to VMware solutions on the IBM Cloud.

Expanded Portfolio of IBM Cloud for VMware Solutions

Today, IBM and VMware each made announcements that further this strategic partnership and support continued adoption of IBM Cloud for VMware solutions:

Adoption of VMware HCX Technologies: IBM is one of the first partners to adopt VMware HCX technologies. HCX technologies deliver seamless interoperability and application mobility between IBM Cloud and any VMware-based cloud, enabling large scale application migration and ongoing portability with zero application downtime or refactoring. HCX technologies will allow IBM Cloud customers to modernize data centers with the most current VMware SDDC offerings while maintaining business continuity, application uptime, network architectures and performance.

VMware Horizon Cloud Service: VMware Horizon Cloud is the next generation of virtual desktop and application cloud services from VMware. The VMware Horizon Cloud service offered by IBM Cloud will be made available in Q4 2017 to customers on the IBM Cloud. Horizon Cloud will be delivered as a fully cloud-hosted service managed end-to-end by IBM or a seamless hybrid solution using on-premises hyper-converged infrastructure to enable new use cases for desktops-as-a-service (DaaS).

Certified Public Cloud Infrastructure for SAP HANA® on VMware on IBM Cloud: IBM today announced the availability of new SAP-certified bare metal servers for SAP HANA® platform deployments in the IBM Cloud and new configurations for VMware environments.

IBM Cloud is Now VMware Cloud Verified: IBM Cloud is one of the first of a new class of partners carrying the VMware Cloud Verified trust mark. VMware Cloud Verified identifies providers that fuel business growth by driving innovation, improving efficiency and lowering costs for customers as they transform application portfolios for a multi-cloud, multi-device world.

New Technology Ecosystem Partners to Provide Network Control and Visibility: To help clients have a consistent experience spanning on-premises environments and the public cloud, IBM is broadening its ecosystem of technology partners and introducing solutions from F5 Networks and Fortinet for full network traffic control and workload security capabilities.

F5 Networks: In Q4 2017, IBM will make F5 Networks' BIG-IP virtual suite of products available in the IBM Cloud for VMware solutions portal. Enterprises will have the ability to order, deploy and configure the F5 BIG-IP virtual edition products for automated integration with VMware Cloud Foundation and vCenter Server on the IBM Cloud. This will offer enterprises the security- rich,

continue on page 94

intelligent network traffic management and application performance optimization for their most critical workloads. Read more in this blog.

Fortinet: In Q4 2017, IBM will make Fortinet's FortiGate-NGFW virtual appliance and bundled services available in the IBM Cloud for VMware solutions portal. Enterprises cannot afford to choose between security and maintaining a high-performance business infrastructure. FortiGate on the IBM Cloud will help maintain secure application availability by extending robust enterprise network firewall functionality into their hybrid cloud environments.

"Enterprises in nearly every industry want to use the cloud to modernise and create new business opportunities," said Faiyaz Shahpurwala, General Manager of IBM Cloud. "IBM's partnership with VMware has enabled more than 1,400 enterprises to quickly and easily transition to the cloud to securely scale and enhance their workloads with full access to a rich catalog of IBM Cloud services, including AI, data and analytics, IoT, serverless and more."

"VMware and IBM are seeing increasing customer momentum as we continue to be strategically aligned in supporting customers' journey to the cloud," said Ajay Patel, senior vice president and general manager, cloud provider software business unit, VMware. "From our early partnership to deliver complete software-defined data centers as a service through VMware Cloud Foundation, and now our pioneering efforts with VMware HCX technologies to reduce the cost and complexity of large-scale on- premises workload migration, together we are delivering a powerful enterprise cloud platform with operational consistency and global scale."

For more information, please visit: www.vmware.com SST

NEC Preempts Stealthy Cyber Attacks and Detects Unknown Attacks

NEC contributes to strengthening cyber security by leveraging its unique AI technologies and specialist organisations for cyber security, through collaborations with partners worldwide, and through its global operation framework

Detecting Unknown Cyber Attacks Through Advanced AI Technologies and Automatically Minimising System Damage

NEC developed the world's first* Automated Security Intelligence technology, which identifies unknown cyber attacks previously not possible to detect. This unique AI-based technology uses autonomous learning to detect unknown cyber attacks in real time from in-house network behavior that is "not normal." Once an attack is detected, the technology automatically identifies the scope of damage and quarantines affected devices. In an unlikely event that systems and facilities sustain an attack, NEC's advanced AI technologies for automatically detecting abnormalities in currently operating systems enable a rapid response and a means to minimise damage.

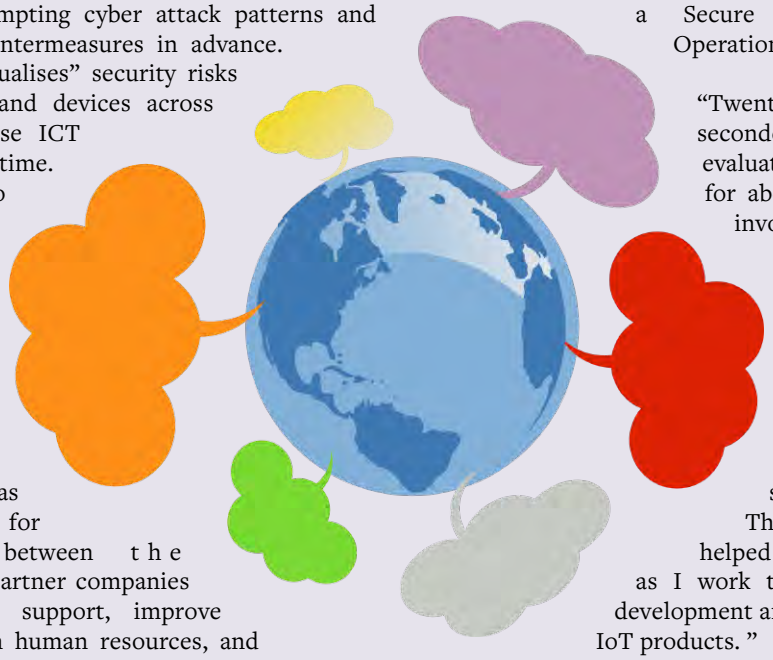
Strengthening Security by Working Together with Worldwide Partners from Inside and Outside the Company

NEC established a specialised organisation to handle cyber security (CSIRT: Computer Security Incident

continue on page 95

"As part of its cyber security business infrastructure in the APAC region, NEC has established a Security Operation Center (SOC) and forged collaborations with INTERPOL, in order to further strengthen its global operation framework for handling cyber security. Going forward, NEC will combine "information/knowledge," "technology", and "human resources," and collaborate with its partners worldwide to contribute to building a safe and secure society."

Response Team) in 2000, through which it has carried out organisational cyber security initiatives, including the monitoring of cyber attacks, analysis of attack methods, investigation of causes, and resolution of incidents. Building on the experience and knowhow gained from these initiatives, NEC offers the NEC Cyber Security Platform that realises "proactive cyber security" by preempting cyber attack patterns and implementing countermeasures in advance. The platform "visualises" security risks in servers, PCs, and devices across the entire in-house ICT system in real time. NEC has also established the Cyber Security Factory (CSF), which gathers experts in cyber security from inside and outside the company. CSF serves as the core facility for collaborations between the NEC Group and partner companies to provide total support, improve technologies, train human resources, and carry out leading initiatives in cyber security.



Also, as part of its cyber security business infrastructure in the APAC region, NEC has established a Security Operation Center (SOC) and forged collaborations with INTERPOL, in order to further strengthen its global operation framework for handling cyber security. Going forward, NEC will combine "information/knowledge," "technology", and "human resources," and collaborate with its partners worldwide to contribute to building a safe and secure society.

Keeping Society Safe from Security Risks in the IoT Era

In the era of IoT, many different things and contexts will be seamlessly connected via networks. A vulnerability discovered in any one of the devices, parts, services and systems that we deliver to our customers could have a disastrous consequence. It is vital that we maintain the highest degree of quality right from the development stage, which is why we have established a Secure Development and Operations Promotion System.

"Twenty years ago, I was seconded to an ISO/IEC 15408 evaluation organisation for about four years. I was involved in evaluating whether companies had implemented an appropriate system for preventing future problems with products or systems from an information security perspective. This experience has helped me tremendously as I work to ensure the secure development and operation of NEC's IoT products. "

NEC considers security for not just its ICT systems but also their IoT products from the design stage, so that they can maintain the highest possible quality.NEC calls this "Security by Design." NEC has also invested considerable resources in staff training so they can help customers by providing them with both state-of-the-art technologies and expertise in secure development and operations. This is just one of the ways NEC is contributing as a company to creating a safer and more secure society.

For more information, please visit:
www.necam.com SST

Introducing Sanbot Nano, an AI Robot for the Home

New Robot Features Amazon's Alexa Voice Service and Smart Home Control

Berlin, Germany – At IFA 2017, QIHAN Technology Company introduced Sanbot Nano, a home assistant robot equipped with Amazon's Alexa Voice Service. Building on QIHAN's success in delivering "robotics-as-a-service" solutions, the intelligent, cloud-enabled robot features voice capabilities via Alexa, smart home control and remote monitoring capabilities, delivering centralised management and security to households around the world. Sanbot Nano currently supports English and German languages and will available for purchase starting in October for $2,800.

"The world is captivated by the emergence of robotic developments and we're constantly challenging ourselves to making the most amazing robot experiences possible," said Ryan Wu, CMO, QIHAN. "With Sanbot Elf's breakthrough growth in the retail, hospitality, public service and government industries, we are excited to introduce a robot for the home. Sanbot Nano's customised capabilities will make every family feel like they have a personal assistant."

Sanbot Nano stands at 2.7 feet tall and is equipped with over 50 sensors to avoid objects in its way, recognise voices and know when someone enters the room. Sanbot Nano is also equipped with advanced features for the home, including:

- **Voice Capabilities:** Through Amazon's Alexa Voice Service, Sanbot Nano can order pizza, request a car, track fitness stats, control the TV, play music from today's leading streaming providers and more.
- **Smart Home Control:** Sanbot Nano pairs with smart home devices from the world's most popular connected home brands, enabling families to control lights, thermostats and home appliances.
- **Remote Monitoring:** QIHAN's mobile Q-Link App allows families to live-stream video and control Sanbot Nano from anywhere in the world.

In addition to Sanbot Nano's new voice capabilities and smart home control features, the new mini robot inherits many popular features from QIHAN's Sanbot Elf including the Android SDK, Sanbot App Store and automatic charging.

For more information, please visit: www.en.sanbot.com/nano.html SST

"Building on QIHAN's success in delivering "robotics-as-a-service" solutions, the intelligent, cloud-enabled robot features voice capabilities via Alexa, smart home control and remote monitoring capabilities, delivering centralised management and security to households around the world."

Has Your Smart Thermostat Been Hacked?

Call for tighter regulations on smart thermostats

If you've got a smart thermostat, you're putting all your trust in the technology to get you the best deal on your heating by using it wisely. But boiler and heating specialists Warm.co.uk have warned that this could be a big mistake.

Warm.co.uk have called for tighter regulations on the heating industry when it comes to smart devices, arguing that they're open to being manipulated by unscrupulous energy companies or even hackers. It's a popular conspiracy theory, but one that's gaining a lot of ground, as customers begin to complain that their smart meters are using more gas and electricity than they think they should be.

Studies have shown that the energy savings smart meters promise can actually decrease over time, in a move some customers are calling a deliberate move to present higher bills. A spokesperson from Warm.co.uk said: "Smart meters are notoriously insecure, leaving them open to potential hackers off all kinds.

Warm.co.uk has heard from a customer who had their smart meter hacked during a house party. After being paired with a party-goers phone, the heating was controlled without the homeowners permission leading to a huge increase in bills, and head scratching. "In theory, anyone who hacked into your smart meter could see what you were using, change your bill one way or the other, and change settings if they know what they're doing.

"Studies have shown that the energy savings smart meters promise can actually decrease over time, in a move some customers are calling a deliberate move to present higher bills. A spokesperson from Warm.co.uk said: "Smart meters are notoriously insecure, leaving them open to potential hackers off all kinds."

"That's without even thinking about what the energy companies could do with your energy consumption if they wanted to." It doesn't just work one way round either. Sometimes energy companies themselves can be the victims, with Warm.co.uk citing one particular example in Puerto Rico during 2009.

Smart meters there were hacked en masse by former employees from a power company in what officials called 'power theft'. Smart meter users were charged an extortionate amount if they wanted to find out how to alter their own energy readings, costing the energy company concerned almost $400million per year. SST

APAC Consistently Ranks on Top Across Multiple Threat Categories in the First Half Of 2017

Globally, ransomware, business email compromise scams continue to plague enterprises; new threats such as fake news and robotics attacks are growing

Singapore – Trend Micro Incorporated, a global leader in cloud security solutions, today revealed that Asia Pacific had been heavily hit from January to June 2017, leading other regions in most threat categories.

Globally, Trend Micro detected 82 million ransomware threats and found that on average, 28 new ransomware families were created every month. The company also blocked more than 3,000 BEC attempts; and discovered and responsibly disclosed 382 new vulnerabilities.

In the meantime, cyberpropaganda reared its head in 2017 – cybercriminals started selling tools and services that helped create fake content, boost social media reach, and buy votes that can directly influence elections. Connected devices continue to be a problem too. In April, Trend Micro discovered the Persirai botnet targeting more than 1,000 Internet Protocol (IP) camera models. The company also found more than 83,000 exposed industrial routers and 28 exposed industrial robots.

"APAC was targeted by threats and cyberattacks disproportionately in the first half of the year. Companies in the region need to better understand cyberattacks and prioritise funds accordingly for effective security." said Dhanya Thakkar, Managing Director and Vice President, Asia Pacific, "Based on the insights we gather, our team has been continually constructing a comprehensive threat intelligence database and innovating new products that can respond to the growing threats. That's why we have started incorporating machine learning-based smart detection technology into all our solutions and gleaned good results."

Key APAC Highlights and Insights:

Out of the 82 million ransomware threats blocked, those targeting APAC entities accounted for 35.7% of all, the highest of all regions. This is followed by EMEA (25.24%), Latin America (22.66%), and North America (15.71%).

The successive successes of WannaCry and Petya attacks reinforced the need for consistent patching for enterprises across all industries. Despite Microsoft releasing a patch in March for the vulnerability CVE-2017-0144 or EternalBlue, which WannaCry and Petya

continue on page 99

exploited, the attacks still infected thousands of computers in April and in June.

Other noteworthy ransomware families that surfaced in the first half of the year included new variants of Cerber, an infamous ransomware now armed with anti-machine-learning capabilities; Patcher, which affected the MacOS; and the mobile ransomware SLocker.

The best defense against ransomware threats is to block them at the source level via web or email gateway solutions. Machine learning technology such as Trend Micro's XGenTM is designed to detect ransomware threats by filtering them through multiple defense methods, eading to effective, comprehensive detection even for newly created, never-seen-before ransomware variants.

- In the first six months of the year, more than 436 million malware detections were observed in the APAC region, surpassing the numbers in all other regions by a huge margin. APAC is followed by North America (324 million) and EMEA (169 million). The top three malware found in the region are DocDrop, DOWNAD, and WannaCry. The most hit countries in the region are Japan, Australia, and Taiwan. As industrial IoT devices continue to mushroom in APAC, the number of supervisory control and data acquisition (SCADA) system vulnerabilities is also increasing, providing fodder for malware attacks. Based on the findings from the Trend Micro's Zero Day Initiative program, there exist malware specially made to target these connected systems. APAC also leads in the number of detections for online banking malware in the first half of the year, culminating in more than 118,193 malware discovered and blocked, four times more than EMEA (24,798) and five times more than North America (20,888). Japan, China, and Vietnam encountered most of the attacks.

- Trend Micro also found that more than 47 million malicious mobile apps were downloaded by users in APAC, much more than those from other regions. For instance, EMEA users downloaded 30 million such apps; the numbers are even lower in North America (eight million) and Latin America (six million).

- Exploit kits are another prominent threat in the APAC region, with a total of 556,542 detected within the six months, more than quadrupling the second place – North America (120,470). The most distributed exploit kits for the first six months in APAC are Rig, Magnitude, Sundown, and Nebula. Exploit kits normally target popular software such as AdobeFlash, Java, and Microsoft Silverlight. In 2017, connected industrial systems became a popular target for exploit kits too. Some of them can be used to deliver ransomware, such as Rig, Magnitude and Sundown.

> "The best defense against ransomware threats is to block them at the source level via web or email gateway solutions. Machine learning technology such as Trend Micro's XGen™ is designed to detect ransomware threats by filtering them through multiple defense methods, eading to effective, comprehensive detection even for newly created, never-seen-before ransomware variants."

For more information, please visit www.trendmicro.com SST

Thought Worthy

"Security in the IoT needs to be as simple as a key that you give to your kid to open the front door, not as complex as millions of keys. Otherwise it becomes more complex to manage the keys than to provide the security itself." *- Stefan Ferber*

CCTV DRONES COMING TO A NEIGHBOURHOOD NEAR YOU

▸▸ *By cctv.co.uk*

New automated technology that could soon be patrolling your neighbourhood

Drones have been the future technology to watch for the past few years, and it looks like we're still not done thinking about their potential, according to CCTV.co.uk.

The versatility of these flying robots has been proven already, with them being roped in to help with tricky aerial film and TV shots, delivery for online orders, and monitoring wildlife without disturbing any creatures.

Now CCTV.co.uk predict that drones could become a part of all our lives in a much more direct and important way – by patrolling our neighbourhoods in search of criminal activity.

Attaching a camera to a drone is one of the most common ways to use these versatile machines, meaning we can capture images from places humans can't easily get to. They're a great way to explore dangerous or remote terrains, but it also means we can see things from the air that it would otherwise require an expensive helicopter to catch.

Nowhere is this more exciting than in the home and business CCTV security sector. Jonathan Ratcliffe from CCTV.co.uk said: "The use of drones for civilian security has

been on the cards for a while, and it's only a matter of time before they're deployed in this way.

"Their compact size, manoeuvrability and low cost make them an excellent security guard for neighbourhoods, where they can keep an eye on things and can follow anyone acting suspiciously – this will be automated and they will learn to fly back to a charging station ready for the next alert"

"If they spot anything, they can help police by sending any important data via bluetooth and adding to the police resources for ensuring domestic security." Drones are already used as part of national security arsenal for military around the world, as well being deployed in hazardous areas.

Japan will see the first domestic security use of drones, with security company Secom releasing a drone that captures security details of visitors including photos of their faces and their car registrations.

As we run headlong towards the age of artificial intelligence, CCTV.co.uk say that drones can even take on some of the responsibility of meeting and greeting your visitors, promising: "Drones can check out any guests before they get to your door, asking them a few questions to work out whether they're friendly, and guiding them to your door only if they come in peace."

For more information, please visit: www.cctv.co.uk. SST

MORE THAN 60 PER CENT OF SINGAPORE-LISTED COMPANIES SCORE WELL ON CYBER SECURITY, ACCORDING TO INDUSTRY'S FIRST CYBER EXPOSURE INDEX

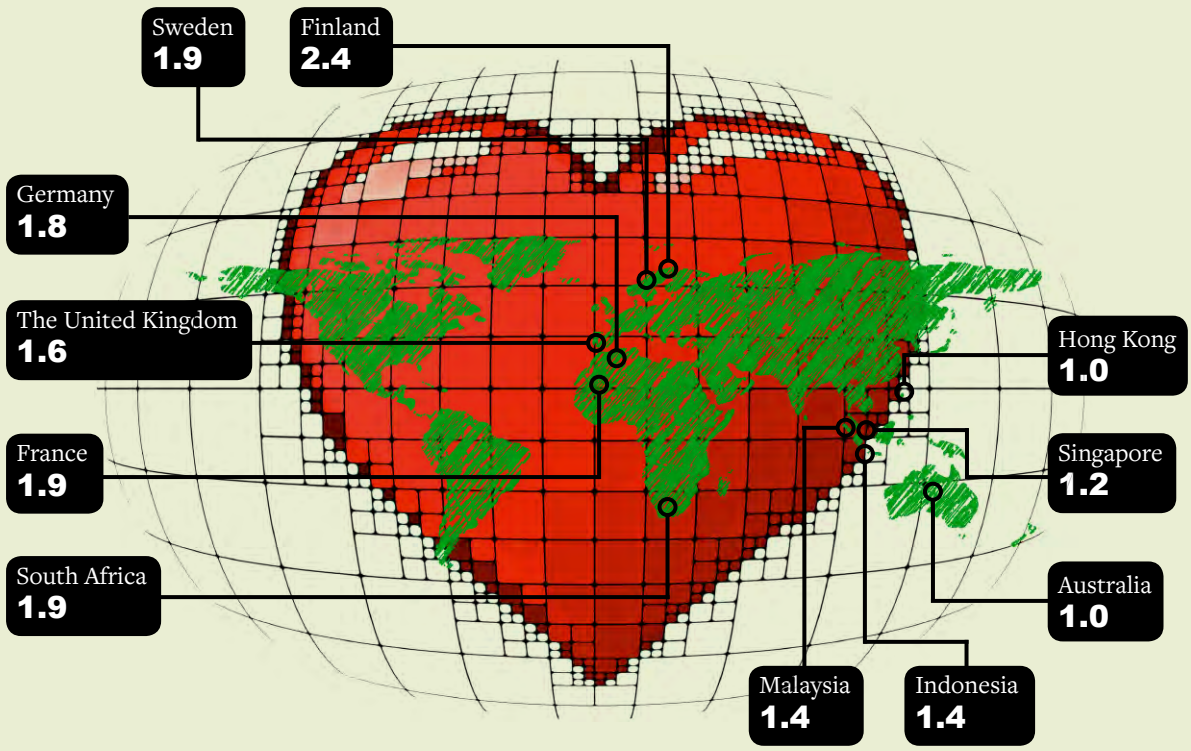
Singapore ranks in the top three countries surveyed in terms of average company cyber exposure

By Kinkayo / RuderFinn

Singapore – Kinkayo, a cyber intelligence company, today launched the world's first Cyber Exposure Index (CEI) – a proprietary global scoring system that evaluates listed companies in a defined and comparable model, based on the number of findings and risk classifications.

Among the 11 markets examined in the Index, Singapore ranks in the top three in terms of average cyber exposure at a country level. Sixty per cent of companies evaluated in Singapore have little or no exposure, compared to the global average of 40 per cent. Other markets identified as leading in cyber security are Hong Kong (74 per cent) and Australia (69 per cent).

Kinkayo collates data from publicly available sources, such as the dark and deep web, and from data breaches, to identify signs of sensitive disclosure, exposed credentials and hacker group activities against companies. The greater



In the case of Singapore, more than six in 10 listed companies have done their due diligence to boost defences and ensure no loopholes in their organisations. By understanding where critical information is stored, from where is it leaking and how it is exposed, companies greatly mitigate the impact of a cyber attack. This is commendable and a right step towards building a transparent business environment.

the amount of uncovered data for a company, the higher the risk and therefore, the higher CEI score. Companies evaluated were given a score from 0 to 5, with 0 equating to no exposure and 5 given to the most exposed companies, based on identified exposure, from September 2016 to September 2017.

In Singapore, 723 SGX-listed companies were evaluated and given scores, with 31.7 per cent given a score of 0 (no exposure) and 30.4 per cent given a score of 1 (little exposure).

Apart from Singapore, the other 10 markets in this study include Australia, Finland, France, Germany, Hong Kong, Indonesia, Malaysia, South Africa, Sweden and the United Kingdom.

Countries ranked based on average company exposure scores (scale of 0 to 5)

Mikko S. Niemelä, President and CEO, Kinkayo, said, "As businesses leverage technology to become more digitalised, they will be challenged with new risks and threats. The reliance on the Internet – the perfect breeding ground for a host of cyber threats – opens doors to vulnerabilities. Companies must employ a proactive and transparent approach to identify these loopholes within their organisations.

Among the 11 markets examined in the Index, Singapore ranks in the top three in terms of average cyber exposure at a country level. Sixty per cent of companies evaluated in Singapore have little or no exposure, compared to the global average of 40 per cent. Other markets identified as leading in cyber security are Hong Kong (74 per cent) and Australia (69 per cent).

"In the case of Singapore, more than six in 10 listed companies have done their due diligence to boost defences and ensure no loopholes in their organisations. By understanding where critical information is stored, from where is it leaking and how it is exposed, companies greatly mitigate the impact of a cyber attack. This is commendable and a right step towards building a transparent business environment."

Data Breaches – What Kind of Data and In Which Industry

According to Kinkayo, the types of company information most at risk is that regarding mergers and acquisitions, databases, intellectual property, registers and business and project plans. The company also identified industries that cybercriminals targeted most often in 2017, and how much data hackers made public.

For all countries evaluated, the biggest exposure tracked was in the manufacturing/industrial sectors.

"As there are more companies overall in this sector, it is expected that a large portion of exposure is in these industries. In addition, many companies in manufacturing may not have adequate security IT investment as compared to financial services or healthcare industries," Mr Niemelä said.

About the Cyber Exposure Index (CEI)

The Cyber Exposure Index was developed to allow for fair and independent comparison of companies worldwide. The CEI is based on data collected from publicly available sources in the dark web, deep web and data breaches. From that data, signs of sensitive disclosure, exposed credentials and hacker group activity against a company are identified. Companies are ranked based on the number of findings and the risk that the findings represent. Approximately 5,000 companies were surveyed in 11 countries and territories globally. These included Australia, Finland, France, Germany, Hong Kong, Indonesia, Malaysia, South Africa, Sweden and the United Kingdom. Data was collected between September 2016 to September 2017.

For more information, please visit www.cyberexposureindex.com. SST

DATA INTEGRATION HELPS SMART CITIES FIGHT CRIME

By Hitachi and Intel® IoT

Hitachi public safety visualisation solutions use Intel® technology to enhance real-time intelligence, situational awareness and investigative capabilities

The goal of Hitachi Visualisation is to help agencies share real-time insights that enhance situational awareness and investigative capabilities when an incident occurs.

Integrating and Analysing Public Safety Data

To better understand and combat criminal activity, today's public safety and law enforcement agencies need to bring together data from various systems, including video surveillance, emergency systems, criminal records, and more. Hitachi Visualisation integrates public safety solutions and makes information easy to share between public and private agencies. Intel® hardware within the Hitachi Visualisation Platform* (HVP*) powers data capture, analytics, and work flow, from edge devices to the cloud and data center. The Hitachi Visualisation Suite* (HVS*) provides software that visually correlates data. These solutions break down barriers that plagued older security information management systems and are leading to exciting new possibilities, like predictive crime analytics.

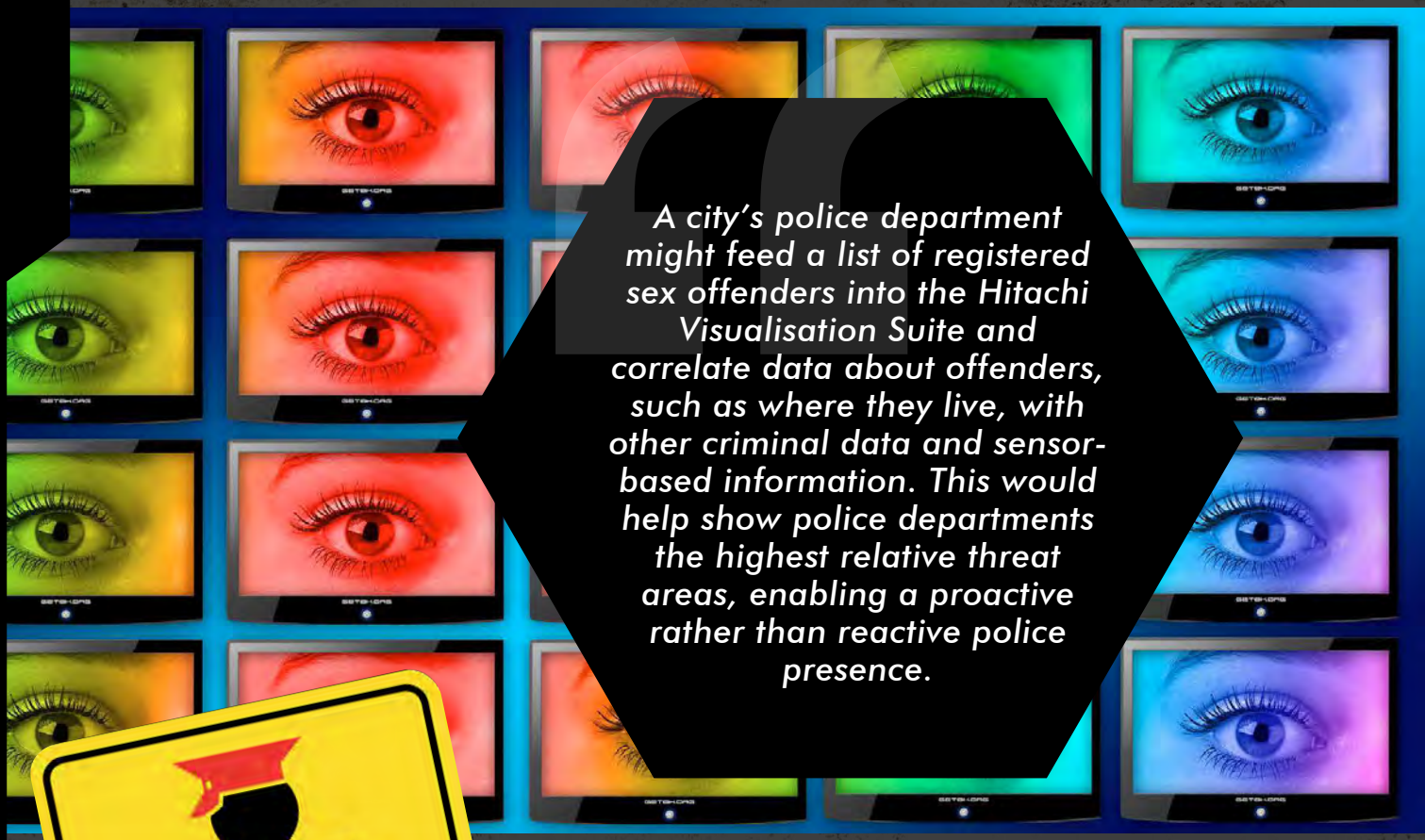
In the event of an emergency such as an active shooter, agencies need to quickly track down and share data from disparate public and private systems. For instance, surveillance cameras posted on private buildings, such as banks, can help identify a suspect. Quick transmission is critical as agencies work to prevent casualties and other damage.

Slow Data Sharing Delays Emergency Response

Today, public safety and law enforcement agencies have more crime fighting tools to work with than ever before: video monitoring systems, computer-aided dispatch (CAD)/911 systems, license-plate recognition devices, gunshot sensors, records management systems, and a range of other evidence-detection solutions.

However, this data is often siloed and difficult to access. In the event of an emergency such as an active shooter agencies need to quickly track down and share data from disparate public and private systems. For instance, surveillance cameras posted on private buildings, such as banks, can help identify a suspect. Quick transmission is critical as agencies work to prevent casualties and other damage.

Harnessing data to fight crime is part of a larger transition to smart cities, in which buildings, railways, buses, airports, areas of traffic, and utilities all need a way to integrate and secure the data they receive from third-party sensors. With fast, secure data integration and analysis, smart cities can take energy management, security, and public safety to new heights.



> *A city's police department might feed a list of registered sex offenders into the Hitachi Visualisation Suite and correlate data about offenders, such as where they live, with other criminal data and sensor-based information. This would help show police departments the highest relative threat areas, enabling a proactive rather than reactive police presence.*

Austin Police Monitor Hotspots for Crime

The City of Austin, Texas, was an early adopter of public safety technology—it won awards when it replaced videotape-based devices in police patrol cars with modern digital cameras. More recently, the Austin Police Department (APD) implemented a real-time observation project based on the Hitachi Visualisation Platform.

As part of its High Activity Location Observation (HALO) initiative, the APD installed edge-capture camera pods in strategic hotspots for crime throughout the city. The camera pods use the Intel® NUC and support:

- Gunshot detection
- License-plate recognition
- Radioactive isotope detection
- Video management systems, access control and radar
- CAD/911systems
- Videoanalytics, intelligent routing, bonding and failover
- Cloud-managed bandwidth monitoring and configuration
- Third-party cameras

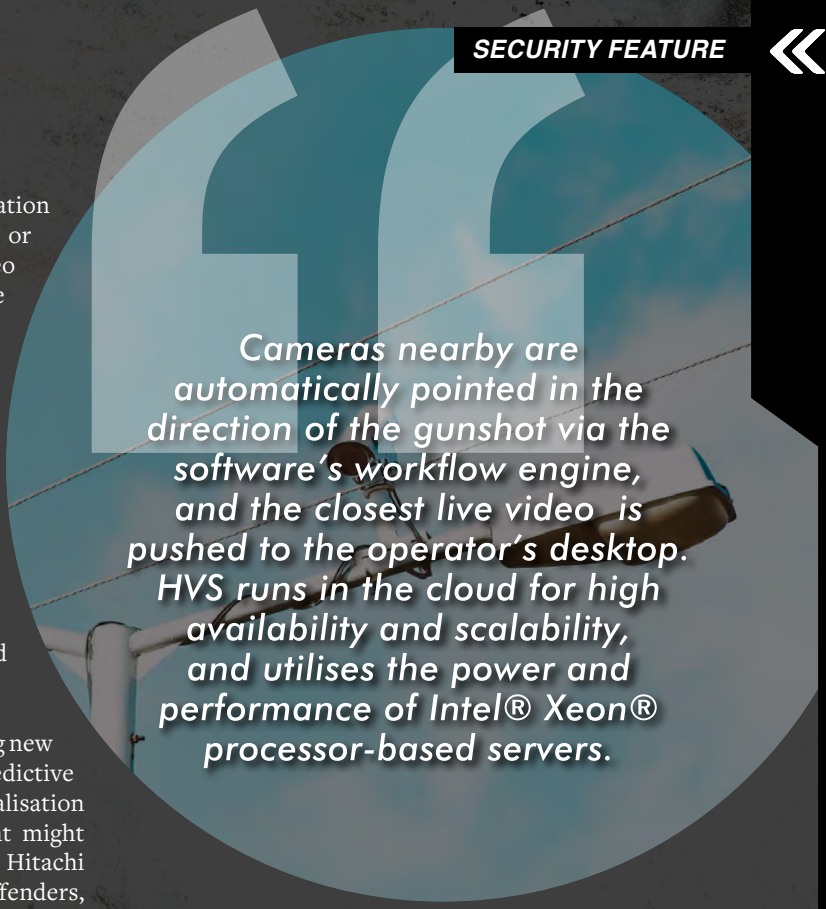
In addition to providing real-time criminal monitoring, HALO has better prepared officers to respond to emergency calls. The camera pods also offered a way for APD to stretch its budget while making a big impact on criminal activity.

Real-Time Insights for Public Safety

Hitachi Visualisation was created to solve two key problems in

public safety. First, agencies need an application that can easily integrate various point systems or public safety solutions, such as third-party video feeds, CAD/911 systems, and gunshot and license plate sensors. Second, the application must be easily accessible to outside agencies for video sharing. The goal of Hitachi Visualisation is to give agencies real- time insights that enhance situational awareness as well as investigative capabilities when an incident occurs. This cloud-based application gives agencies a single pane of glass for video and data sharing. So far, Hitachi has deployed visualisation solutions in major cities in the Caribbean and across the United States, including Washington, D.C.; Austin, Texas; and Atlanta, Georgia.

The ability to correlate data is leading to exciting new possibilities. In 2015, Hitachi launched a predictive crime analytics platform as part of its visualisation suite. For example, a city's police department might feed a list of registered sex offenders into the Hitachi Visualisation Suite and correlate data about offenders, such as where they live, with other criminal data and sensor-based information. This would help show police departments the highest relative threat areas, enabling a proactive rather than reactive police presence.



Cameras nearby are automatically pointed in the direction of the gunshot via the software's workflow engine, and the closest live video is pushed to the operator's desktop. HVS runs in the cloud for high availability and scalability, and utilises the power and performance of Intel® Xeon® processor-based servers.

Hitachi Visualisation

Hitachi Visualisation is an integrated hardware and software solution. The Hitachi Visualization Platform encompasses the hardware devices used for edge capture, analytics, and work flow:

Camerapods are integrated camera and communication devices that can be easily deployed on city poles and building infrastructure. The camera pods quickly and securely transmit high-definition video and data straight to the cloud.

Gateways integrate third-party video systems and perform transcoding for live cloud streaming and recording. Gateways also serve as a data ingest service for sensor data. Small form factor gateways feature an Intel® CoreTM i7 processor for powerful processor and graphics performance at the edge.

Hitachi's Video Management Platform is a hyper-converged compute and storage appliance hosted by Intel® Xeon® E5 processor-based servers. It's optimised for video management storage and retrieval, allowing the solution to consume large amounts of video streams and store them on the premise or in the cloud. It's also certified on many of the largest third-party video management systems in the video surveillance market.

A variety of transmission options including cellular 4GLTE and wireless mesh or point-to-point are ideal for wide area deployments. Hitachi Visualisation Suite provides the software for visually correlating ingested data and video. For example, when a gunshot is detected, the event is shown on the map. Cameras nearby are automatically pointed in the direction of the gunshot via the software's workflow engine, and the closest live video is pushed to the operator's desktop. HVS runs in the cloud for high availability and scalability, and utilises the power and performance of Intel® Xeon® processor-based servers.

Better Data for Safer Cities

Hitachi Visualisation's latest public safety solutions can help agencies connect and correlate data, resulting in smarter and safer cities. Intelligent edge-capture devices make it possible to rapidly deploy and manage robust communication networks across wide areas, while cloud-based software enhances actionable intelligence.

Hitachi Visualisation breaks down the barriers that traditionally plague older physical security information management architectures by leveraging the ubiquitous nature of the Internet and software as a service (SaaS) deployment model. It's an intelligent model for forward-thinking cities, made possible by the performance and edge-to-cloud scalability offered by Intel IoT solutions.

For more information, please visit: www.hds.com. SST

PUBLIC SAFETY AND THE INTERNET OF THINGS

By Kova Corp

The Internet of Things is one of the most exciting technological developments since, well...the internet.

If you're not familiar with this concept, all it refers to are objects – from toys to electric meters to watches – that are connected to the internet. There are plenty of these items connected and in use already. Most of those that have gained a lot of attention are in the private sector: the Amazon Fire TV Stick, for example, and the Apple Watch are both part of the Internet of Things (IoT).

While the public sector is also starting to use the IoT in interesting ways, public safety organisations are really only just beginning to take advantage of the IoT and the many possibilities it offers. Those that are, however, are finding that the IoT presents them with all kinds of opportunities. Check out some of the recent developments in this area below.

> *The device connects other devices already used by first responders – body cameras, heart rate monitors, public safety drones, and other sensors – and allows the first responders to share that information with command posts and other relevant parties.*

Wearable Gateway for First Responders

The winner of the 2016 IJIS Institute Innovation Award, the Internet of Public Safety Things Wearable Gateway is a wearable communications gateway for first responders. The device connects other devices already used by first responders – body cameras, heart rate monitors, public safety drones, and other sensors – and allows the first responders to share that information with command posts and other relevant parties.

The device can transmit multimedia information, making it useful for all branches of public safety. According to a press release by Mutualink, the company that developed the gateway, potential uses for the device include:

- Communication of biosensor data from firefighters, to aid in prevention and early detection of exhaustion or distress
- Live streaming from police officers' body cameras
- Managing multi-location crises, with SWAT teams transmitting real-time location data to a command center during active shooter or terrorist situations

Cloud-Based Platforms for Predictive Policing

Predictive policing involves the use of analytics, technology, and/or mathematics to identify potential areas or instances of crime before they occur. One company, Hitachi Data Systems, has released a tool called Predictive Crime Analytics that uses real-time social media and internet feeds, along with analytics, to help police make predictions.

According to DataCenter Dynamics, this tool is the first to tie information from social media and the internet together with analytics. The platform is part of the Hitachi Visualisation Suite, which brings together data and video from various public safety systems.

Like Physical Security Information Management technology, this kind of data integration tool can greatly improve law enforcement's situational awareness, as well as provide the real-time information that can help prevent incidents from becoming crises.

ShotSpotter

ShotSpotter is a new technology that uses sensors mounted in high crime areas to identify the sound of gunfire (you can read about how this technology is being integrated into smart streetlights here). These sensors not only identify the sound of shots, but also pinpoint their location, analyse the sound, and then send all of that data to connected police stations and PSAPs within one minute.

One company, Hitachi Data Systems, has released a tool called Predictive Crime Analytics that uses real-time social media and internet feeds, along with analytics, to help police make predictions. According to DataCenter Dynamics, this tool is the first to tie information from social media and the internet together with analytics.

ShotSpotter has been deployed in many cities around the country, and according to news reports, it has been successful in lowering rates of gun crime. In Wilmington, N.C., for example, gun crime has been reduced by 2 percent, while homicides have decreased by 20 percent, since the city installed the technology. In addition, police response time to gunshot incidents has gotten faster.

As public safety organisations continue to embrace the possibilities of the Internet of Things, cities will continue to become safer places to live and work. Public safety technology can help make PSAP, command post, or security system more efficient and effective and KOVA is one such company offering these solutions.

For more information, please visit: www.kovacorp.com. SST

LIP READING CCTV

COMING TO A SUPERMARKET NEAR YOU

Read Our Lips: CCTV Will Soon Hear Us Without Sound

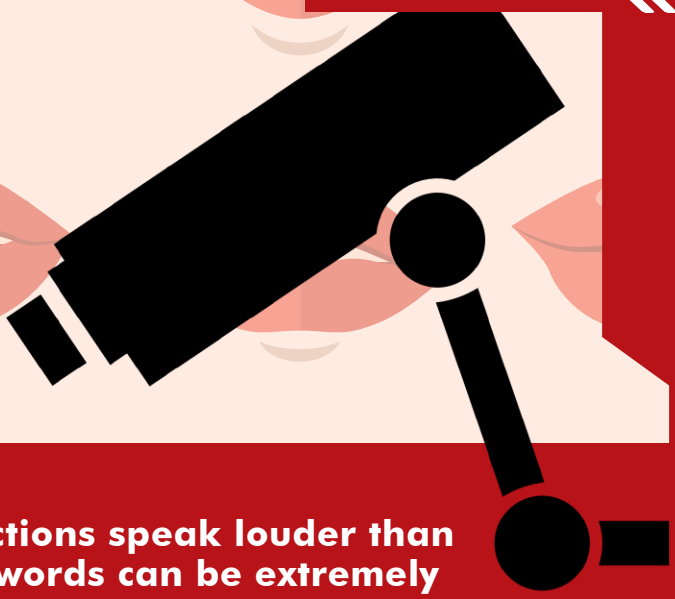
►► *By cctv.co.uk*

UK - Lip-reading cameras open up possibilities for revolutionary market research - and you can't escape. They say actions speak louder than words, but words can be extremely important too, which can sometimes makes silent CCTV footage a bit useless.

However, UK-based security experts CCTV.co.uk say that's all about to change, because they're predicting the imminent rise of lip-reading cameras and software. "Visual speech recognition technology has been in development for some time," said a spokesperson from CCTV.co.uk, "and it's almost ready to be unveiled in the next generation of CCTV systems."

"This new tech will read lips and give you an idea of the words being spoken in the images it captures. While we generally associate this type of functionality with interpreting what contentious things were said by players at football matches, it has far wider reaching implications, especially for business."

Without the accompanying dialogue, some incidents caught on camera at your store remain a mystery, because your cameras



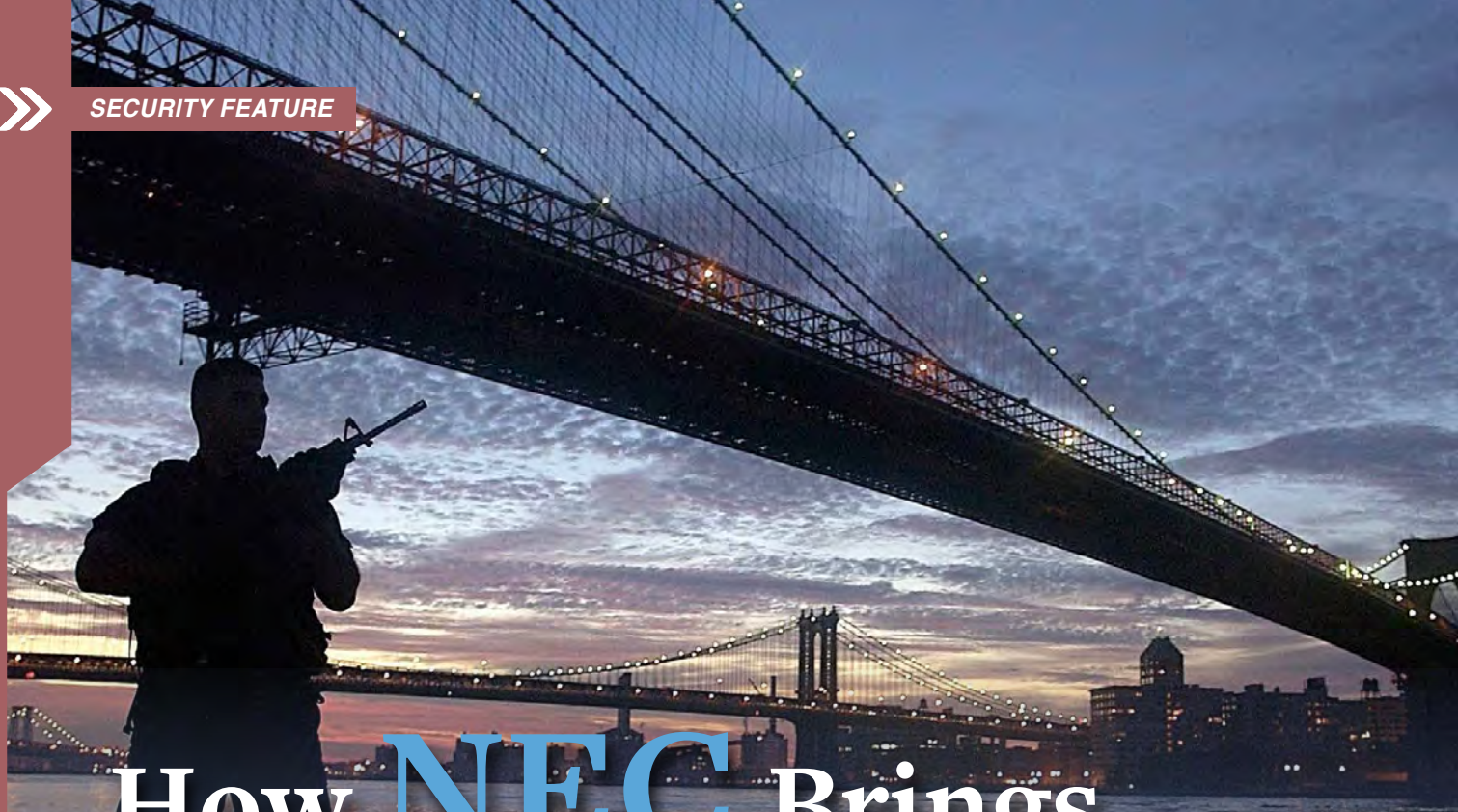
"They say actions speak louder than words, but words can be extremely important too, which can sometimes makes silent CCTV footage a bit useless."

don't have microphones that can pick up the sound. That's fine when it comes to things like catching shoplifters, although it's next to useless for finding out what your customers really think of your store, services or products.

But soon, systems will be able to capture and relay just what customers are thinking, without having to chase them down with a pen and a page full of tick boxes. A spokesperson from CCTV.co.uk explained: "If you're a business wanting to know your visitors' opinions, a survey relies far too much on their honesty and effort to fill it in. "With this leap in CCTV technology, businesses can analyse their customers' reactions to a particular aspect of their store or service, and get qualitative as well as quantitative data. By capturing the comments of customers this way, they get an insight into unedited and genuine information that couldn't be captured any other way.

"Of course this new camera technology will be particularly useful in noisy environments, for example. But many business premises play music or have multiple conversations happening at once, so there's no escaping it."

For more information, please visit: www.cctv.co.uk. SST



How NEC Brings Cutting Edge Security to Smart Cities and Public Spaces

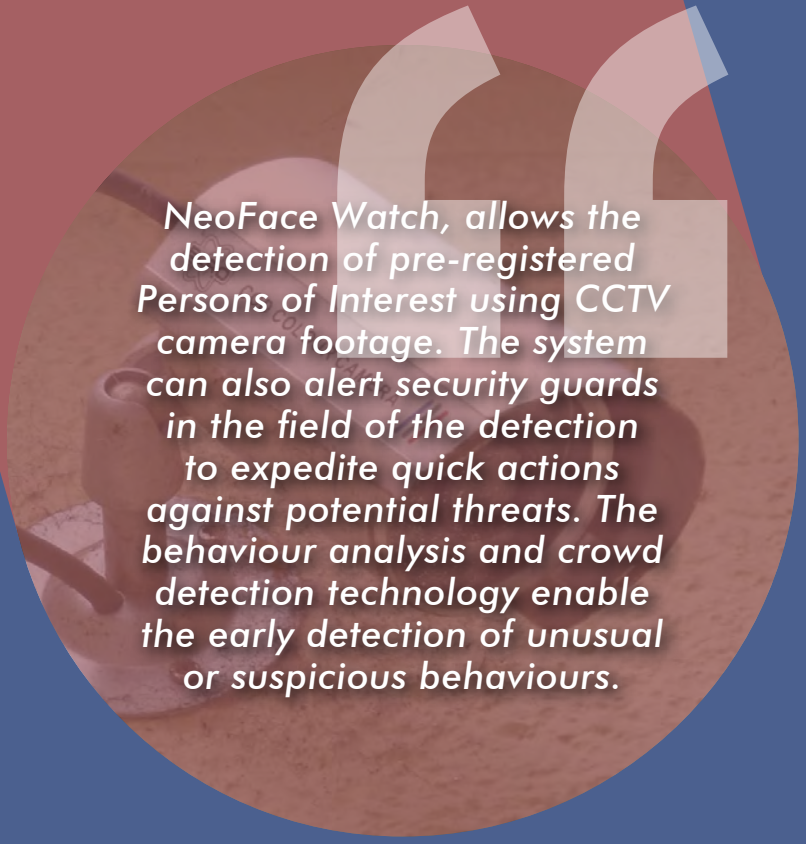
By Cate Lawrence writing for readwrite.com

One of the most interesting things about emerging technology is seeing traditional companies bring their years of experience to solve social problems for the greater good. An example is the work of Japanese company NEC who contribute to the development of smart cities and public safety with the use of cutting-edge technologies. I visited them at Mobile World Congress this year in Barcelona to learn more.

Smart Cities and Public Safety

NEC's booth exhibited Cloud City Operation Centre (CCOC), an IoT platform that provides support for urban management. CCOC is operating in a number of locations including Santander, Spain and Wellington, New Zealand to simulate efficient and optimal management of urban resources by introducing visibility into data that is collected from the city.

"NEC's Cloud City Operation Center combines information from a multitude of sensors and data sources, geotags that data and then further enriches it with metadata and analytics for use by many different vertical applications," explains Tim Packer, Head of Smart City Solutions at NEC New Zealand. "NEC is also partnering Wellington in its Living Lab project, through which the city seeks to explore how smart city technology can improve



> *NeoFace Watch, allows the detection of pre-registered Persons of Interest using CCTV camera footage. The system can also alert security guards in the field of the detection to expedite quick actions against potential threats. The behaviour analysis and crowd detection technology enable the early detection of unusual or suspicious behaviours.*

community wellbeing and the safety of its citizens.

"In this project, existing data sources and assets, coupled with new sensory and analytical methods and technologies, offer insights into day-to-day street level trends, patterns and hotspots. This provides the agencies and city partners with the real-time information they need to alert and respond to issues as they arise and to assist informed decision making around social initiatives and policy to keep Wellington safe and vibrant."

NeoFace Watch

NEC also demonstrated their premier face recognition technology and crowd density quantification solution. The real-time face recognition solution, NeoFace Watch, allows the detection of pre-registered Persons of Interest using CCTV camera footage. The system can also alert security guards in the field of the detection to expedite quick actions against potential threats. The behavior analysis and crowd detection technology enable the early detection of unusual or suspicious behaviors.

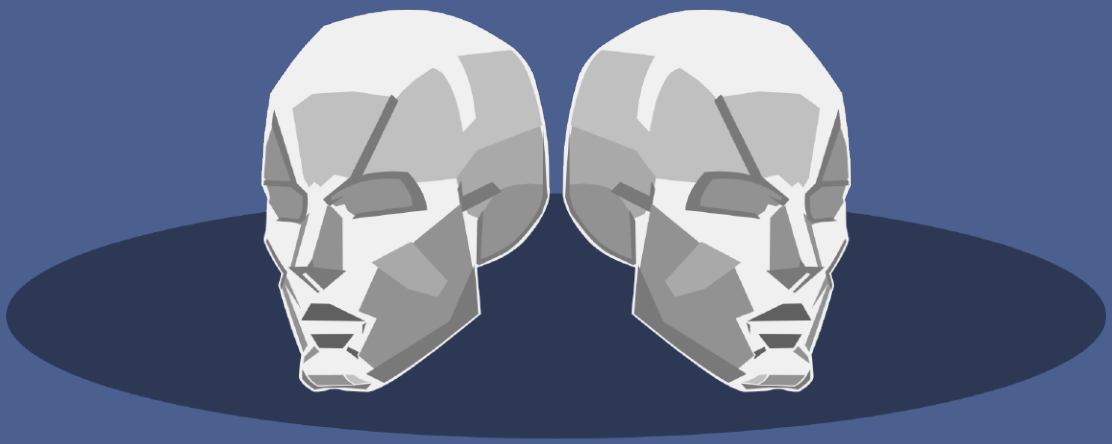
The NeoFace Watch is specifically designed to integrate with existing surveillance systems by extracting faces in real time from existing video surveillance systems and matching against a watch list of individuals. When the system identifies an individual of interest from the watch list, it raises an alert, so appropriate actions can be taken rapidly to reduce the risk of public safety threats.

Crowd behavior monitoring

Using the advanced techniques of the company's unique machine learning video analytics technologies, NEC can trigger alerts when crowd behavior video surveillance indicates potentially illegal, undesirable or anti-social activity.

The benefits include the ability to tacitly maintain and appropriate the level of surveillance that optimizes operations staff attention to the most important or critical situations. NEC's video surveillance solution to detect and analyze crowd behavior in real time has been introduced at Tigre in Argentina.

It can also spot dangerous drivers and suspicious vehicles, the detection of double-riding on a motorcycle, a common form of purse snatching, and license plate recognition to quickly identify stolen cars. Many people visit



Tigre from both inside and outside the country, and on weekends the population of the city almost triples compared with weekdays. Because of this, improving the fundamental infrastructure of the city to solve problems related to the high volume of traffic and the high crime rate was an issue that needed to be addressed urgently so that both citizens and tourists could feel safe and secure.

It was also vital to construct a management system that would allow the efficient integration of information to reduce incidents and accidents and improve public order, and also allow quick coordination between public organisations, including the police. This solution has successfully reduced vehicle theft by 80% from 2008 to 2013.

NEC has installed over 500 safety and security related systems in 40 countries around the world and will continue to provide unique local solutions to local problems.

Harbor Monitoring Network System

Another interesting piece of infrastructure by NEC is the Harbor monitoring system, a threat detention service. It uses various types of sensors installed both on land and underwater to detect, track, and monitor small suspicious ships and divers — including those with underwater scooters — who trespass upon important facilities along the coastline.

The ITV, hypersensitive camera, and infrared camera automatically search the target area in response to information about suspicious objects detected by radar. The system also uses multiple sensors installed on the ocean ¬floor to detect and track divers invading underwater and small suspicious submersibles that cannot be detected by radar. Like the radar information, information about suspicious objects is sent to the ITV, hypersensitive camera, and infrared camera, which automatically search the target area to capture images of divers or submersibles when they surface.

Information obtained by this system can be sent to related organisations, surveillance ships defending the periphery, other surveillance vehicles, and defense personnel via various types of networks such as wireless LANs. It can also be used as an environment monitoring system to detect potential disasters such as radiation and tsunamis.

The system also uses multiple sensors installed on the ocean ¬floor to detect and track divers invading underwater and small suspicious submersibles that cannot be detected by radar. Like the radar information, information about suspicious objects is sent to the ITV, hypersensitive camera, and infrared camera, which automatically search the target area to capture images of divers or submersibles when they surface.

It is inevitable that as the development of smart city applications grows, the opportunity for utilising technology for crime deterrence, prevention, detection and ultimately prosecution will grow. Such efforts are not new or unique, but are simply being made more successful through technological advancements.

Understandably, few citizens like the ideas of being easily surveilled in public spaces. But citizens also like the idea of crime prevention and detection. The challenge is how the nexus between these two competing ideas can be successfully navigated. If the work of NEC is anything to go, future life in the cities will get even more interesting.

For more information, please visit : www.nec.com. SST

This article was originally published at www.readwrite.com and has been used with permission.

Smarter Surveillance for Safer Cities:

THE FUTURE OF VIDEO-SUPPORTED LAW ENFORCEMENT

By Bosch Security

One global mega trend that will endure through 2017and beyond is urbanisation. Cities continuously attract more and more people ultimately looking for better opportunities and better lives. With ever-swelling urban populations come increasing development challenges. One key challenge for urban planners is rising insecurity, as stated in the World Cities Report 2016, released by the UN-Habitat: http://wcr.unhabitat.org

To ensure that growing cities remain or become better places to live, city governments and law enforcement authorities must tackle the issue of insecurity. Modern security systems provide help in fighting violence and crime more efficiently; especially the latest technological advancements in the digitalisation of video surveillance technology, which contribute to making cities safer, smarter and more sustainable.

Smart Gunshot Detection

The value of new IP video security surveillance technology in stemming violence and crime is immense. It is a first-line defence that not only allows authorities to gather essential evidence to help solve crimes, but also to anticipate certain security issues before they become a problem. Despite the growing number of video cameras installed in cities, the immediate challenge once a gun has been fired has always been to capture a reliable view of the perpetrator. That is, until now.

The latest Bosch PTZ cameras allow authorities to instantly locate and zoom in on a gunshot or explosion, enabling them to immediately identify the assailant and assess the surrounding environment in high detail. Having access to such information enables law enforcement to analyse a situation more accurately and to take immediate action when every second counts.

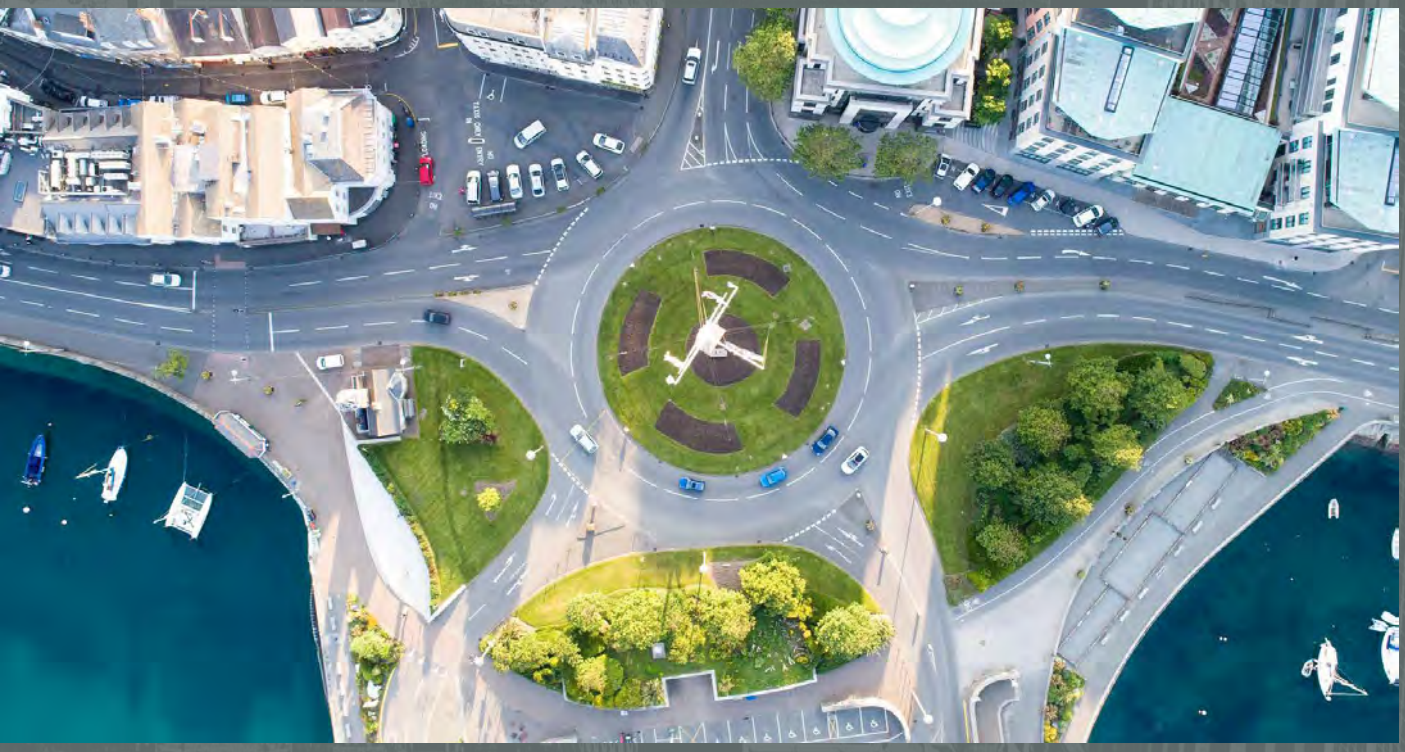
This is possible with gunshot detection systems. Based on the neurobiological principles of brain signal processing, gunshot detection technology allows, like the human brain, accurate

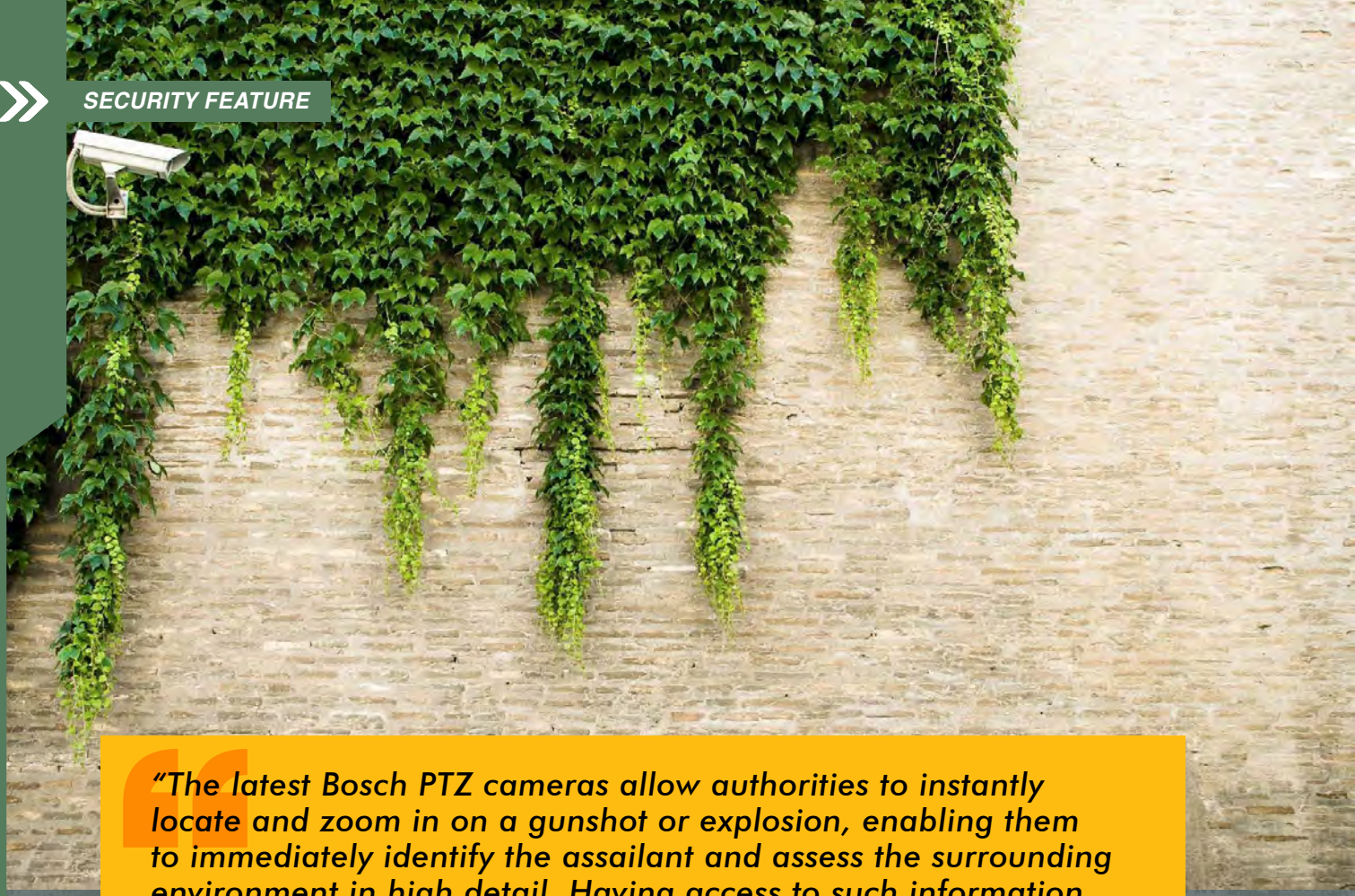
"To ensure that growing cities remain or become better places to live, city governments and law enforcement authorities must tackle the issue of insecurity. Modern security systems provide help in fighting violence and crime more efficiently; especially the latest technological advancements in the digitalisation of video surveillance technology, which contribute to making cities safer, smarter and more sustainable."

recognition of acoustic signals even in the presence of high noise. It is capable of distinguishing sounds and determining the location of the source. With this technology, surveillance units are able to immediately zoom in on the source of the noise, while the camera's auto-tracking functionality enables users to track the perpetrator.

Another benefit of this technology is the reduction of costly false alarms when noises are caused by other, benign sources such as fireworks.

A gunshot detection system can be integrated with Bosch AUTODOME IP and MIC IP 7000 series PTZ cameras. These cameras deliver detailed images even in fog and rain or other difficult weather conditions. They are capable of identifying the darkest and lightest parts of the image, which in foggy conditions are different shades of grey. They then set the darkest grey to black and the lightest grey to white, thus increasing contrast. Finally, the cameras adjust each of the RGB colours to improve colour





"The latest Bosch PTZ cameras allow authorities to instantly locate and zoom in on a gunshot or explosion, enabling them to immediately identify the assailant and assess the surrounding environment in high detail. Having access to such information enables law enforcement to analyse a situation more accurately and to take immediate action when every second counts."

saturation and therefore overall image quality.

Another issue faced by surveillance in urban areas is the passing of large freight traffic vehicles or trains which can shake cameras and cause destabilisation. This can also be an obvious problem in the event of an explosion; a new image stabilisation algorithm helps solve this problem: it detects continuous vibration and dynamically corrects the shaky video in both vertical and horizontal axes. The result is a stable image on the monitor – with no reduction in camera sensitivity.

Smarter Street Lighting

City planners are tasked with not only creating safer urban environment, but also smarter ones to reduce energy costs. Striking a balance between good video surveillance and efficient outdoor lighting is not always a straightforward task.
Bosch's solution is to combine video surveillance and street light dimming – not only by deploying new IP video cameras but also, in many cases, by adapting existing IP surveillance cameras already installed in urban areas. Many streets and inner city areas are already equipped with Bosch video surveillance cameras to help protect people and property. These cameras often have Intelligent Video Analysis and are mounted on lampposts. Through Bosch's various power line Ethernet (Minos, Uvax) and wireless (Paradox) partnerships, it is now possible to link these cameras with video analytics to street lighting systems - not only for the lamppost on which the camera is mounted, but also for other lampposts in the same street. Once this link has been established, the cameras are able to pass on information to other cameras on the street to enable light dimming.

In times when there are no passers-by, lighting is dimmed by 20%. Once movement is detected, the camera's algorithm determines the size; for cats, dogs, foxes and other small animals, the lighting remains dimmed. However, when a person, cyclist or car is detected, the lighting level is increased. Based on the speed and direction it becomes possible for the illuminated area to 'follow' the movement. After a pre-determined period without motion, the lights are dimmed again.

The results are cost effective, yet smart, efficient lighting that ensures the safety of passing pedestrians, cyclists and motorists. Moreover, the network cameras use the same electrical power supply as the lamppost. These cameras also make use of the available infrastructure to transmit video, either wired via the power line, or

> *"...city planners can add more temporary cameras to enhance safety as and when necessary – for example on occasions that attract large crowds of people such as concerts, festivals and sports events."*

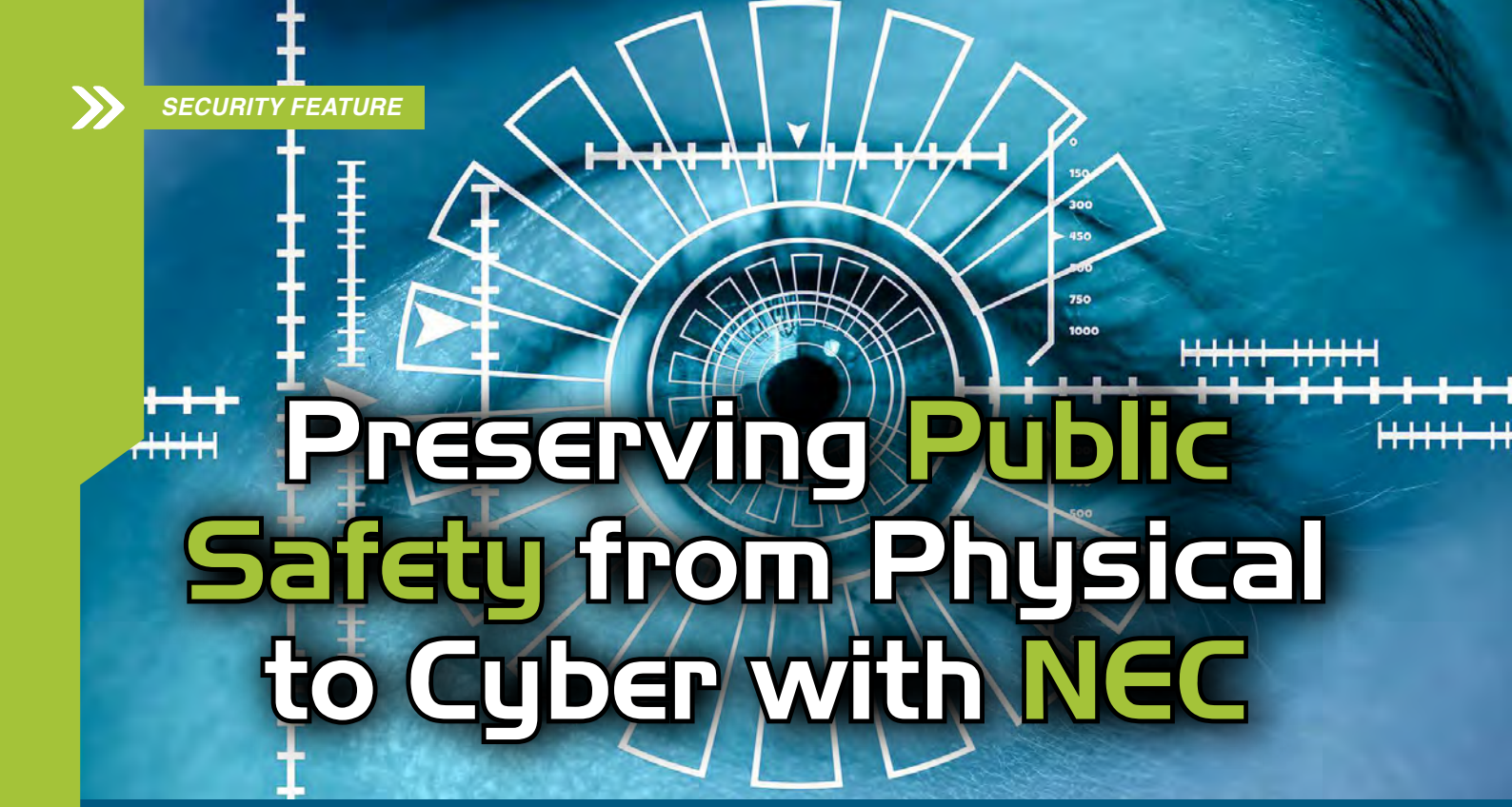
wireless using WiFi, therefore, no new cables are needed, which also saves on installation costs.

This means that city planners can add more temporary cameras to enhance safety as and when necessary – for example on occasions that attract large crowds of people such as concerts, festivals and sports events.

Significantly reducing the lighting level can make it difficult for a camera to detect and analyse motion. This is why some Bosch camera models incorporate 'starlight' technology combining a new class of sensor and the latest Intelligent Dynamic Noise Reduction technology. The result is not only motion detection but also clear images for accurate analysis, retro-analysis and lighting control, even in extreme lowlight conditions.

Urban centres around the world will continue to grow. The latest advancements in smart security technology can significantly contribute to making our urban spaces safer and at the same time, more sustainable places to live.

For more information, please visit: www.boschsecurity.com SST



Preserving Public Safety from Physical to Cyber with NEC

By NEC

Globalisation and advancement of IoT have led to the rise of various kinds of threats to daily life and society.NEC supports safety and security through cutting-edge, world-class AI and biometrics technologies. NEC Levevrages AI, biometrics and other cutting-edge technologies to deliver advanced safety.

Increasing Threats From Crime, Natural Disasters and Cyber Attacks

The world today faces many challenges: threats to society from crimes and terrorist acts, threats from natural disasters such as earthquakes and tsunamis, and threats from cyber attacks that are becoming increasingly stealthier and more sophisticated. Global population and urbanisation will continue to increase, and by 2050, it is forecasted that 70% of the world's population will be living in cities. As national and regional borders fade with the advancement of urbanisation and globalisation, maintaining public order and ensuring the safety and security of infrastructures will become more critical than ever. Moreover, the need for measures to protect cities and lives from natural disasters caused by global warming and from large-scale earthquakes and tsunamis will become more pronounced.

Meanwhile, as new social values are generated through the "connectivity" brought about by the advancement of Internet of Things (IoT) that links people and things of all sorts, allowing us to more deeply understand contexts, this connectivity also brings with it an increase in security risks. Today, we are seeing an uptick in cyber attacks and organised crimes perpetrated by specialised groups. These attacks not only cause damage in the cyber world through the infiltration of information and communications technology (ICT) systems, such as data loss or falsification and theft of information assets, but also bring threats of physical damage into the real world (physical world) as seen by increasing incidents of unauthorised entry into facilities and acts of terrorism. As the advancement of IoT continues, it is clearer than ever that we will need both physical and cyber safety measures to protect our social infrastructure and ensure that it runs stably.

> "NEC has a unique array of technologies for detecting abnormalities in social infrastructures and predicting failures in critical facilities, as well as for quickly detecting suspicious behavior, congestion states and unusual phenomena in public spaces. These technologies make cities safer by preventing incidents and accidents before they happen."

Making People and Society Safer and More Secure Through A Physical-Cyber Security Approach

NEC leverages its sensing and surveillance technologies to visualise people, things and environmental changes in the real world and then analyses the collected data by using artificial intelligence (AI). This data is converted into information from which new knowledge can be obtained and applied to the real world to prescribe actions there. NEC has a unique array of technologies for detecting abnormalities in social infrastructures and predicting failures in critical facilities, as well as for quickly detecting suspicious behavior, congestion states and unusual phenomena in public spaces. These technologies make cities safer by preventing incidents and accidents before they happen. NEC also offers the world's most accurate* biometrics technologies that are deployed in many countries and regions around the world, delivering reliable results for their users.

In the field of cyber security, NEC carries out advanced initiatives in developing security measures for preempting cyber attacks, detecting system abnormalities, and automatically detecting unknown cyber attacks using AI technologies. NEC is also reinforcing cyber security
measures through the establishment of a core facility specialising in cyber security and through the global deployment of safety solutions catering to worldwide needs. Going forward, through alliances with cyber security vendors and collaborations with international agencies and partners worldwide, we will continue to strengthen our cyber security operation frameworks, develop human resources, and enhance our solutions and services.

Detection of Threats to Social Infrastructures and Critical Facilities

> "One of NEC's solutions is Crowd Behavior Analysis, a technology that detects congestion and unusual phenomena from surveillance videos in real time, while maintaining personal privacy. Crowd Behavior Analysis can be used to prevent crime, and also to respond quickly and guide residents to safety in an emergency or disaster."

NEC reinforces physical security for protecting people and social infrastructures from accidents, incidents, and natural disasters through AI and biometrics technologies, and technologies for detecting earthquakes and tsunamis.

Protecting People and Society Through Advanced AI and Biometrics Technologies

Through its world-leading AI technologies, NEC is continually pursuing the evolution of its advanced and diverse physical security solutions. For public spaces, such as cities, airports, and stadiums, NEC prevents the occurrence of accidents and incidents through early detection of dangerous behavior and suspicious vehicles from video surveillance images. One of NEC's solutions is Crowd Behavior Analysis, a technology that detects congestion and unusual phenomena from surveillance videos in real time, while maintaining personal privacy. Crowd Behavior Analysis can be used to prevent crime, and also to respond quickly and guide residents to safety in an emergency or disaster.

Further, NEC's Fingerprint Identification, Face Recognition, and other biometrics technologies, which are ranked as the world's most accurate, are widely used in many countries around the world in applications ranging from national level security, such as national ID systems and airport immigration systems, to personal identification in enterprises and facilities. NEC is also establishing a global framework for providing its safety solutions to all regions around the world to enhance its safety business.

Protecting People from Natural Disasters Through Reliable Earthquake and Tsunami Observation Systems

NEC has more than 20 years experience in developing systems for the Japan Meteorological Agency that provide immediate information on earthquakes and tsunamis. These cutting-edge
systems instantaneously process and analyse the epicenter and scale (magnitude) of an earthquake based on data received from measuring instruments to allow authorities to issue earthquake early warnings, earthquake-related information, and tsunami warnings. We also provide total support for laying down deep-sea cables and constructing earthquake and tsunami observation systems, including the provision of optical submarine cables, seismometers/ tsunami meters, repeaters and other equipment.

For more information, please visit: www.necam.com SST

ABOUT PIXEL DENSITIES AND WHAT THEY MEAN

▸▸ *By Vlado Damjanovski, B.E.(electronics & TV)*

An IP surveillance system may be used to observe and protect people, objects and people's activity inside and outside the objects, traffic and vehicles, money handling in banks, or games in casino environment. All of these objects of interest may have different clarity when displayed on a workstation screen. The image clarity depends primarily on the camera used, the imaging sensor, its lens and the distance from the object.

There is one parameter in IP CCTV that expresses the image clarity in a simple way with just one parameter - Pixel Density. The Pixel Density is usually expressed in pixels per meter (Pix/m), at the object plane, although it can be expressed in pixels per foot. Pixel Density in IP CCTV sense should not be confused with the Display Pixel Density quoted by various LCD display manufacturers which defines the screen density, in Pixels Per Inch (PPI).

The advantage of expressing object clarity with its Pixel Density is that it combines the sensor size, pixel count, focal length and distance to the object in just one parameter.

When using Pixel Density metrics all variables are included and makes it universally understandable what details you will get on an operator's workstation screen.

When designing a system, or a tender for a system, one can request Pixel Density for a particular image quality. So, instead of asking for a 6 mm lens for your camera in a particular location, for example (which means nothing without knowing the camera sensor it is used on), it would be much more useful if a particular Pixel Density is defined for the view. This will then be used to calculate the required lens for the particular camera used and the distance from the object. This will guarantee the clarity of the image (assuming the lens is focused optimally and there is sufficient light, of course). Pixel Density can be used for any object that IP CCTV user might be interested in: face, licence plate, playing card, money and similar.

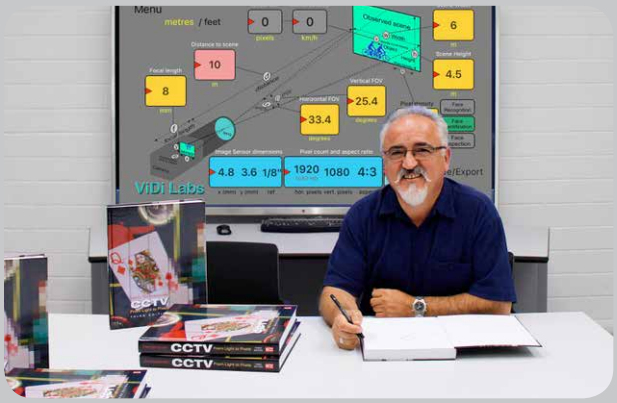
Let us now explore how many pixels per meter are attributed to various objects.

Vlado Damjanovski

With over 35 years of professional experience, Vlado Damjanovski is one of the world foremost experts and authority in Closed Circuit Television. He is an author, inventor, lecturer and closed circuit television (CCTV) expert based in Sydney, well known to the International CCTV industry.

Through his company ViDi Labs he provides training, consultancy, design, product testing and publishing.

Vlado has a degree in Electronics Engineering from the University "Kiril & Metodij" in Skopje (Republic of Macedonia), specialising in Broadcast TV and CCTV. His 1982 thesis on the subject of Charge-Coupled Devices (CCD) preempted their wide commercial use by ten years.



In 1995 Vlado published his first technical reference book - simply called 'CCTV'. This was, and still is, one of the first and complete reference manuals on the subject of CCTV. Covering all that a CCTV expert, installer and consultant should require, this book was accepted and approved by the international industry. Now in its 4th edition and translated into four languages, Vlado's book continues to have a 5-star rating. The last edition is titled 'CCTV - from light to pixels' and it is translated into multiple languages, including German, Russian, Korean and Farsi.

Utilising his best-seller books Vlado conducts easy-to-understand CCTV training seminars. He demystifies and explains all the tricks and technologies of the CCTV industry. These seminars are conducted worldwide (www.cctvseminars.com).

In addition, Vlado has designed and commissioned a number of CCTV Systems around Australia and overseas. These include large-scale projects such as the Darling Harbour CCTV system, the Downing Centre CCTV system and the Sydney City Council system. In 1997 Vlado was the chief consultant and designer for the Star City Casino Pit-Cam CCTV system, one of the very first digital CCTV systems in the world using digital recorders.

Vlado was the publisher of the foregone magazine 'CCTV Focus'. This magazine was launched at the International Security Conference (ISC) in New York, August 1999. 'CCTV Focus' became the leading technical magazine for the CCTV industry.

Through his company, Vlado designs and offers many specialised CCTV tools for the industry. These tools include Programmable Test Pattern Generators, Camera Analysers, CCTV Test charts, ViDiLabs iOS calculator App, system drawings icons and tools.

Vlado was the chief contributor in the creating of Australian and New Zealand CCTV Standards (AS4806.1, AS4806.2 and AS4806.3).

Vlado is now an active member of IEC TC-79 group contributing towards the international standards development of 62676 standards for the IP CCTV and VSS.

One of the most commonly referred pixel densities is for Face Identification. Face Identification in CCTV means sufficient clarity of the image so that one can positively identify who the person on the screen is.

According to Australian Standards AS4806.2, for Face Identification in analogue CCTV, we require 100% person's height to fit on the monitor screen display. The details of 100% person's height on a screen have been tested many times and it's been verified that they are sufficient for such a person to be identified. We know that PAL signal is composed of 576 active TV lines, so, according to AS4806.2, a person's height would occupy all of the active lines to make it 100%. Head occupies around 15% of a person's height, which is equivalent to around 86 lines (576 x 0.15 = 86.4), which is the same when converted to pixels (assuming recording is made full TV frame mode, which is equal to two TV fields).

If we agree that an average person height is 170 cm, the head would occupy around 25 cm of that. The Pixel Density at the object, which is required to make a positive Face Identification according to AS 4806.2, can be calculated to be 86 pixels at 25 cm of head height. Since there are 4 times 25 cm in 1 m of height, this becomes 4 x 86 = 344 pix/m. So, one can say that with pixel density of 344 pix/m at the objects plane it should be possible to positively identify a face, according to AS4806.2.

Some other standards may require different values, and one such (newer) standard is the IEC 62676-4, which defines 250 pix/m to be sufficient (i.e. suggests that with slightly lesser pixel density than the AS standards one should be able to identify a person).

Clearly, this number is not fixed in concrete, and it will depend on the observing ability of the operator, as well as other parameters (lens quality, illumination, compression artefacts, etc...), but the key is to understand that such a Pixel Density can be calculated for any type of camera, irrespective if that is SD, HD, 4k or any other format.

The next image quality down, as defined by the standards is for Face Recognition. The details of Face Recognition image should be sufficient to recognise the gender of a person, what he/she is wearing and possibly make an assertion of who that person might be, if picked from a bunch of people that have already been identified somewhere else (e.g. passport or drivers license photo). This is basically an image with half the pixel density to the Face Identification, which according to AS4806.2 should be around 172 pix/ m, while IEC62676-4 suggests 125 pix/m.

The details of Face Recognition image should be sufficient to recognise the gender of a person, what he/she is wearing and possibly make an assertion of who that person might be, if picked from a bunch of people that have already been identified somewhere else (e.g. passport or drivers license photo).

Similarly, pixel density can be defined for vehicle license plates visual recognition (not software automatic LPR). In the AS 4806.2, this is defined as 5% characters height on a display screen, which is around 30 TV lines (pixels) (to be very accurate 576 x 0.05 = 28.8). If we assume that a typical Australian number plate has characters of around 90 mm in height, than this equates to 11 x 30 pixels = 330 pix/m. The number 11 is obtained from dividing 1000 mm (1 m) with 90 mm. One may say that for visual license plates recognition similar pixel density is required as for face identification.

When money and playing cards are observed in banks or casinos, many practical tests have shown that at least 50 pixels are required across the notes or cards longer side in order to positively identify the values. Standard playing cards dimensions are B8 according to ISO216 standard, which is 62 mm x 88 mm. So, we need the 88 mm card length to be covered with at least 50 pixels for proper identification. This means around 550 pix/m (1000 mm / 88 mm = 11 => 50 pix x 11 = 550 pix/m) should be sufficient for playing cards. We may require slightly better pixel density for identifying money, since notes size is typically larger than playing cards, so if one takes the Face Inspection pixels density of 1000 pix/m, it should attain pretty good identification, although as it can be seen from the real life example below, even 770 pix/m might be sufficient.

As it can be concluded from the above examples, the Pixel Density can be defined for any object and any camera, large or small.

The beauty of the Pixel Density parameter is, as said at the very beginning, that includes all parameters influencing the clarity of the observed objects.

For this reason, ViDi Labs has developed the ViDiLabs iOS calc (search the iTunes App Store under "ViDiLabs calc"), a unique tool for the surveillance industry, which can also be used in cinematography, photography and any other imaging application dealing with objects details.

So the following table can be used as a rough guide for various pixel densities. SST

Technology is the Key to Securing Singapore the SMART Nation

Safeguarding through Surveillance

Following the success and immense effectiveness of Police Cameras (Polcams) being installed in2,500 locations, public areas are next on the list as part of efforts to keep Singapore safe. Public areas selected will include densely populated areas such as town centres, hawker centres, link walk ways and other places that see a large volume of people passing through on any given day.

The first phase of Polcams were installed in residential neighborhoods from 2012. The 65, 000 cameras assisted local police in solving over 1, 900 cases due to the 3, 800 pieces of video footage retrieved and reviewed by law enforcement.

Crimes such as theft, outrage of modesty and unlicensed harassment by moneylenders were just some of the cases that were solved thanks to the trusty PolCams 1.0. Follwing this success was the Polcam 2.0 which was introduced in June 2017. The camera boasted brand new features such as pan-tilt zoom functions and even a 360 degree field of view that assisted the police in detecting anomalous events thus proving law enforcement with the full picture. Adding to the already impressive line-up were video analytics capabilities including facial recognition.

Upgrading the Art of Surveillence

This security effort is highly supported by the local government with Prime Minister Lee Hsien Loong calling for better technology and surveilence systems in his recent National Day Rally speech. He cited the 2013 Little India riots as an example claiming that there were too few CCTV cameras which led to reliance on public footage via social media in order to gather evidence. The PM said that in spire of the increased amount of CCTV's in public now, there is a need to gather better data and utilise it effectively.

Mr Yaniv Peretz the Programme Director of Certified Counter Terrorism Practitioner, highlighted the importance of using camera data proactively, rather than in a reactive way. New technologies for CCTV such as facial recognition, video analytics and even people counters developed by companies like Innotec and Axis Communications will assist the authorities in detecting red flsag patterns, predict and prevent criminal behaviour and much more.

"Surveillance videos can capture the process of a terror incident and key evidence, such as the perpetrators and weapons used, and even the routes taken, as well as the extent of destruction and harm to persons and properties," said National University of Singapore

November / December 2017 • Security Solutions Today 125

Sociologist Tan Ern Ser. He added that what makes camera footage an important tool in combating terror is its efficiency in exposing threats and that incidents can be captured in real time, thereby enabling quick responses and more targeted arrests, in addition to assisting injured victims.

> *"Surveillance videos can capture the process of a terror incident and key evidence, such as the perpetrators and weapons used, and even the routes taken, as well as the extent of destruction and harm to persons and properties,"*

Live Footage Indisputable in a Court of Law

Criminal lawyer Rajan Supramaniam was quoted as saying that Camera footage cannot be disputed as it is objective evidence and a visual tool that can capture the essence of an incident which can also be viewed over and over again. He added that the mere presence of cameras could also serve well to deter crime and discourage criminals from committing a criminal act in the first place.

With effective IP cameras and analytic tools, law enforcement agents will now have a front row seat to a crime in progress which will be useful in crime prevention as well.

Policing Neighborhoods with Polcams

One local neighbourhood being protected by Polcams is Sengkang. The crime rate has declined significantly here thanks to the implementation of the Community Policing System (COPS) and the installation of Polcams. This effective two pronged approach to law enforcement involved the installation of over 2, 000 Housing Development Board (HDB) buildings as well as multi story carparks.

Utilising Technology to Fight Crime

Singapore law enforcement personnel are currently involved in projects that will utlise technology to keep citizens safe. These include

> *"Force-wide systems such as the Body Worn Cameras (BWC) and In-Vehicle Video Recording System (IVVRS) are currently being utilised by the local police force. The BWC is a new recording gadget where officers are positioned on the frontline to enhance their crime-fighting capabilities. The IVVRS involves installation of cameras on police vehicles to provide situational awareness of the external surroundings around the vehicles."*

amongst other efforts such as:

PolCam

Police Cameras (PolCam) distribution continues to achieve good progress. Since the project started in April 2012, 62,000 cameras in around 10,000 public apartment blocks and multi-storey car parks under the PolCam 1.0 rollout plan, have been installed. PolCam has provided valuable footages which has assisted law enforcement in solving over 1,100 cases. The programme is currently being expanded with PolCam 2.0, which is the installation of cameras to public areas in town centres, neighbourhood centres, hawker centres and walkways leading to transportation nodes such as MRT stations and bus interchanges. About 11,000 more cameras will be progressively installed over the next few years at 2,500 locations islandwide. 5100 Polcam 2.0 cameras will be rolled out by end of 2017.

Body Worn Cameras and In-Vehicle Video Recording System

Force-wide systems such as the Body Worn Cameras (BWC) and In-Vehicle Video Recording System (IVVRS) are currently being utilised by the local police force. The BWC is a new recording gadget where officers are positioned on the frontline to enhance their crime-fighting capabilities. The IVVRS involves installation of cameras on police vehicles to provide situational awareness of the external surroundings around the vehicles. It will also be able to "live" stream videos from the vehicles back to Command Centres. More than 400 patrol vehicles were fitted with IVVRS as of June 2017.

MCN2

MHA Communications Network 2 (MCN2) is the new radio communications system implemented to support the operations of SPF, SCDF and SAF. The system comprises of various sub-systems such as the Trunked Radio System (TRS), Digital Multi-Channel Recorder (DMR) and network security systems. As the existing SPF's incident management capabilities rely on the accessibility and dissemination of real time information, a private and dedicated wireless broadband network is required to overcome the problem of Telco congestion during major events like IISS, SEA Games, National Day Parade, GE, F1, Christmas, etc. Currently, the police are exploring and trying out the LTE Technology to allow reliable and stable video streaming for near real-time situation awareness. SST

EXCERPTS FROM S.M.A.R.T POLICING FOR SMART CITIES

By © 2015 Ernst & Young LLP

The ability of technology to drive dramatic productivity improvements in an economy is now well-established. With technology continuing to become smarter and cheaper, the application of ICT solutions has also grown. Today, we are increasingly able to create, manage and store large datasets – or "big data." We can collect data that makes it possible to track and predict the behavior of people and systems in ways that were not possible just a few years ago.

Traditional Policing

In ancient Egypt, early guards and watchmen may have been, at least in part, purely local answers to security concerns. They may have been employed by private persons and local institutions such as temples or rich landowners. During the Middle and New Kingdoms, however, a nationwide police force grew out of the semi-military units securing the borders.

Modern Policing

With the passage of time, population increased and so did sophisticated crimes and criminals. Blue collar crimes, pro t-driven crimes and organised crimes rose in the 20th century. The focus of policing was not only to prosecute the individual but also to prevent the crime. Efforts were made to provide Information, Communication and Technology (ICT) solutions to the police force and significantly increase their efficiency.

A range of technologies is used to gather, store, retrieve, process, analyze, and transmit information. Relevant ICT may range from systems installed in public environments over PC-based systems in offices, to systems installed in cars and mobile systems used on-site. In addition to systems that are specifically designed for the police, ICT in use by the general public may offer the police new means of carrying out their tasks.

> *"The degree of city security, measured in terms of the security of intellectual, social, technical, environmental, cultural, leisure and financial capital, can be based on crime, disaster and accident; all of which can be of internal or external origin."*

Modern policing includes the use of CCTV surveillance, radio frequency identification, e-identification, online verification for passport, etc. Modern police is dependent on ICT systems to be more efficient and effective.

The degree of city security, measured in terms of the security of intellectual, social, technical, environmental, cultural, leisure and financial capital, can be based on crime, disaster and accident; all of which can be of internal or external origin.

Smart Policing

Every year, the UK's Metropolitan Police spends around £250 million on running its ICT, most of which is used to maintain outdated, ineffective and overly expensive systems. Smart policing can be defined by the use of modern technology and processes, which increases the efficiency and effectiveness of the policemen on the field. It should include real-time data, social media communication, field tablets, predictive policing tools, and several other options.

Smart policing is important in cities of future, i.e., smart cities. The smart cities can be defined by the presence of smart infrastructure including smart grids for power and water, effective waste disposal mechanism, green transport and modern policing methods. Smart cities extensively use ICT for all services and provide seamless transactions to citizens from one department to other. Greater ICT usage increases the risk to citizens' information, governments' data and business' plans. In a smart city, policing is not limited to safeguarding infrastructure but also includes safeguarding data and information.

> *"Smart policing can be defined by the use of modern technology and processes, which increases the efficiency and effectiveness of the policemen on the field. It should include real-time data, social media communication, field tablets, predictive policing tools, and several other options."*

Smart Cities and Their Security Risks

Smart cities are going to be the reality for municipalities around the world. These cities will use communication networks, highly distributed wireless sensor technology, and intelligent management systems to solve current and future challenges, and create new services. The key features of smart cities can be defined as:

Smart Governance: Flexible governance structure, technology enabled decision mechanisms, smart regulation to connect city laws to new digital realities, and innovation clusters to create jobs and vibrant economies

Smart Economy: Viable and sustainable business opportunities and the presence of innovative enterprises, clubbed with quality education and infrastructure to provide better economic status to the city

Smart Environment: Management of waste disposal in cleaner ways, maintaining pollution free air, water treatment plants to provide a cleaner and greener environment to citizens

Smart Living: Technologies to integrate and analyse massive amounts of data to provide better living to citizens in the form of childcare facilities, community libraries, entertainment modes, hospitals according to area needs, etc.

Smart People: Services, notifications and information to citizens, such as where to find a parking spot or a new local shop or even to monitor air pollution; connect citizens to local government and encourage more

direct participation, interaction, and collaboration

Smart Mobility: Extensive and efficient public transportation network, park and ride, diffusion of ecological cars, limited traffic areas, cycle paths, bike and car sharing

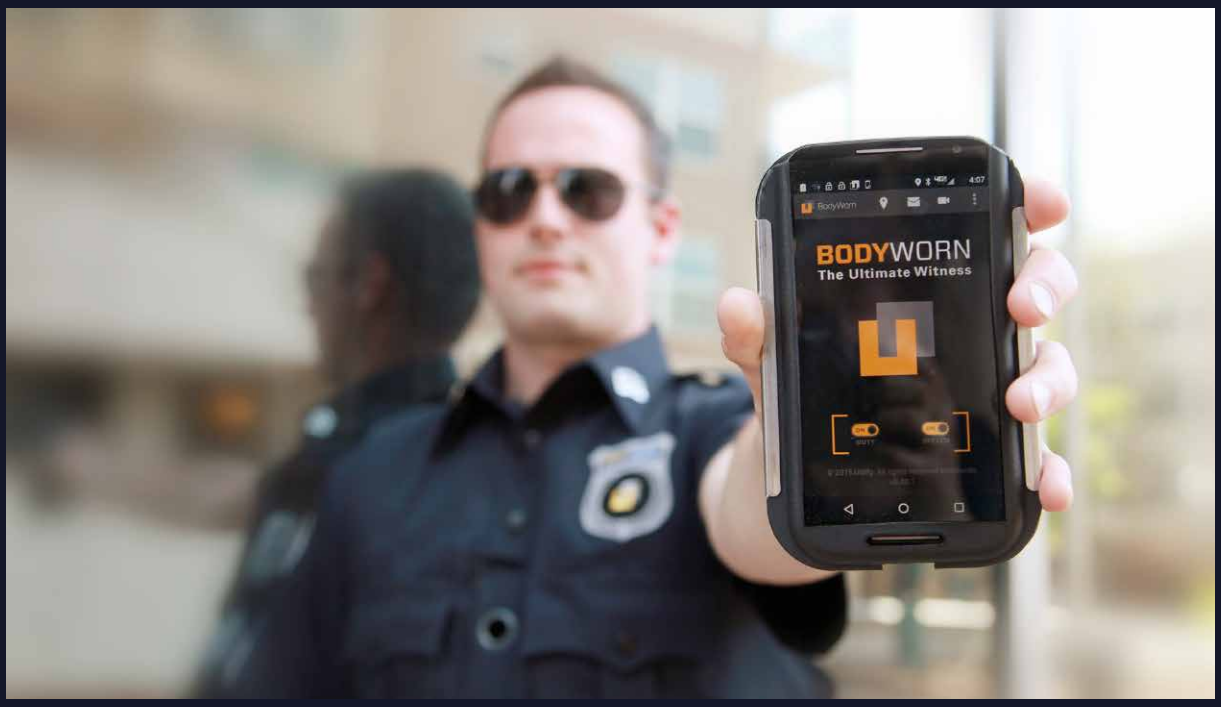
Changing Lives of Citizens in Smart Cities

A typical day of smart citizens could look like this. They wake up on a regular working day, take a look at their smartphone or tablet, and explore a mobile app to choose the best route to go to work. They check train, bus and subway schedules. They also check the temperature, pollution level and weather conditions (based on which they make simple decisions such as packing an umbrella or a jacket.

Sensors everywhere are feeding city systems and these are sending the data to mobile apps. Let's say the person chooses to go by car as there was a delay in public transportation. On their way to work, they check a mobile app for the best route to avoid traffic and another app to select parking based on availability and pricing. Traffic flow is good because of smart traffic control systems that adjust traffic lights based on current traffic conditions. Because of rainy weather, smart street lighting will leave street lights on until there is more daylight. If rain causes floods, food detection sensors will immediately alert the city management and citizens. The city management closely monitors the entire city with the help of surveillance and traffic cameras. The rain causes public transport delays, and information on delays is pushed out so people can choose transport alternatives.

Smart citizens are interconnected via smartphones and gadgets. Smart energy meters, security devices and smart appliances are being used in many cities. Homes, cars, public venues and other social systems are now on the path to full connectivity, known as the "Internet of Things (IoT)." Standards are evolving for all of these potentially connected systems. To benefit from them, city infrastructures and services are changing with new interconnected systems for monitoring, control and automation. Intelligent transportation, public and private, will access a web of interconnected data from GPS location to weather and traffic updates. Integrated systems will aid public safety, emergency responders and disaster recovery.

Smart cities are vulnerable to risk due to their interconnected nature. Attacks can be made to any point of the infrastructure and network. In addition to the primary network, the city data centers catering to the various domains would also be open for exploitation in the event of a security attack. Numerous cyber attacks in the cyber domain have been launched in recent years against the computing infrastructure of various governments. These have been aimed at undermining



> *"As digital citizens become increasingly connected with data available about their location and activities, privacy seems to disappear. Privacy protecting systems that gather data and trigger emergency responses when needed are technological challenges that go hand-in-hand with the continuous security concerns."*

the functioning of information systems, theft of information, or denial of service. These threats have multiplied in today's networked Internet of Things (IoT) paradigm, where machine-to-machine (M2M) interfaces have increased.

With computing systems, the core of security and privacy concerns is the information handled by the system. The three general areas to be secured are:

- The "privacy" and confidentiality of the information
- The integrity and authenticity of the information
- The availability of the information for its use and services

Risks in Smart Cities

Traditionally, risks have been associated with the physical damage caused by the attack. However, with emergence of integrated IT environment, any attack on smart city or citizens of smart city, the attack is not just of physical nature. A modern Indian city embodies people, knowledge, resources, finances, democratic and political aspects, and cultural values. These constituent elements can be classified as asset groups or capital, including intellectual, social, technical, environmental, cultural, leisure and financial capital. Attack can be made on any constituent of the city and can impact socially, economically and emotionally in addition to physical damage.

Risks include illegal access to information, and attacks causing physical disruptions in service availability. As digital citizens become increasingly connected with data available about their location and activities, privacy seems to disappear. Privacy protecting systems that gather data and trigger emergency responses when needed are technological challenges that go hand-in-hand with the continuous security concerns.

For the smart city, the technical target and the related consequence, such as injury to property, personality, life and limb, or emotional damage, must be viewed jointly and, in turn, mapped to the nature of the motivated offender.

First, the victim/target's privacy is heavily compromised because access to vehicle systems provides the offender with near-complete information on where, when and for how long the victim/target has visited a particular location. This privacy violation is a major security risk. Once motivated offenders have a profile and location on the victim/target at all times, they know when that victim/target would be most vulnerable to a physical attack.

Catastrophic failures may also occur because highly connected systems can suddenly fail from a critical point coming under pressure or from a convergence of operations that create a new central point of weakness or a vulnerable target for malevolent action against the company's or government's operation. New threats to systems controls in smart grid, smart water supply/distribution or smart transportation, etc., widen the threat spectrum beyond data protection and software failures. There are risks from any inability of a facilities management process to access its building control systems or to see the systems data on operation of essential services (energy control, access control, communications, unauthorised devices on the system, unauthorised access across systems).

Countering Risks by Smart Policing

The dynamic, changing threats evolving from design, commissioning, operation and change management stages in such a city all require solutions and risk-based decisions within a coherent and harmonious security framework. They also require evaluation of the threat landscape, the safety, security and integrity of systems and people within this landscape, and how business can manage through uncertainties.

Along with risk assessment, smart policing is an aspect that can immensely contribute to the prevention and control of risks arising from these connected people, infrastructure and systems.

Cities are at a point where smart policing is more of an imperative than a mere need.

Countering Risks by Smart Policing

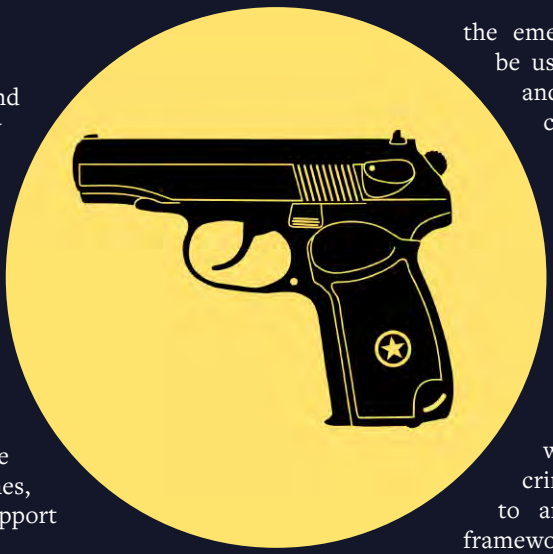
The dynamic, changing threats evolving from design, commissioning, operation and change management stages in such a city all require solutions and risk-based decisions within a coherent and harmonious security framework. They also require evaluation of the threat landscape, the safety, security and integrity of systems and people within this landscape, and how business can manage through uncertainties.

Along with risk assessment, smart policing is an aspect that can immensely contribute to the prevention and control of risks arising from these connected people, infrastructure and systems. Cities are at a point where smart policing is more of an imperative than a mere need.

"Intelligence-led policing is a concept that involves a number of factors coming together. It has been defined as "a business model and managerial philosophy where data analysis and crime intelligence are pivotal to an objective, decision-making framework that facilitates crime and problem reduction, disruption and prevention."

Reliable and Responsive

The diversity of safety and security challenges faced by smart cities means the police force must plan holistic safeguarding measures. Solution providers are moving away from standalone products and systems toward networked solutions, which cover the entire security concept and are more reliable. The police force needs to become reliable and responsive to reduce crimes, improve confidence and support victims.



Multiple Input Mechanism for Emergency Response System

In smart cities, multiple input mechanisms should be available to connect with emergency response services of the police. The input mechanisms may range from phone calls, text messages, emails, voice over IP, messengers, IoT alarms, etc. Facilities to cater to differently abled people should be built in to the new emergency response system. Easy data transmission and critical information sharing can significantly enhance decision- making, and the response and quality of service provided to emergency callers. Messages, photographs and videos received by the emergency response system can be used later for judicial purposes and to create awareness among citizens.

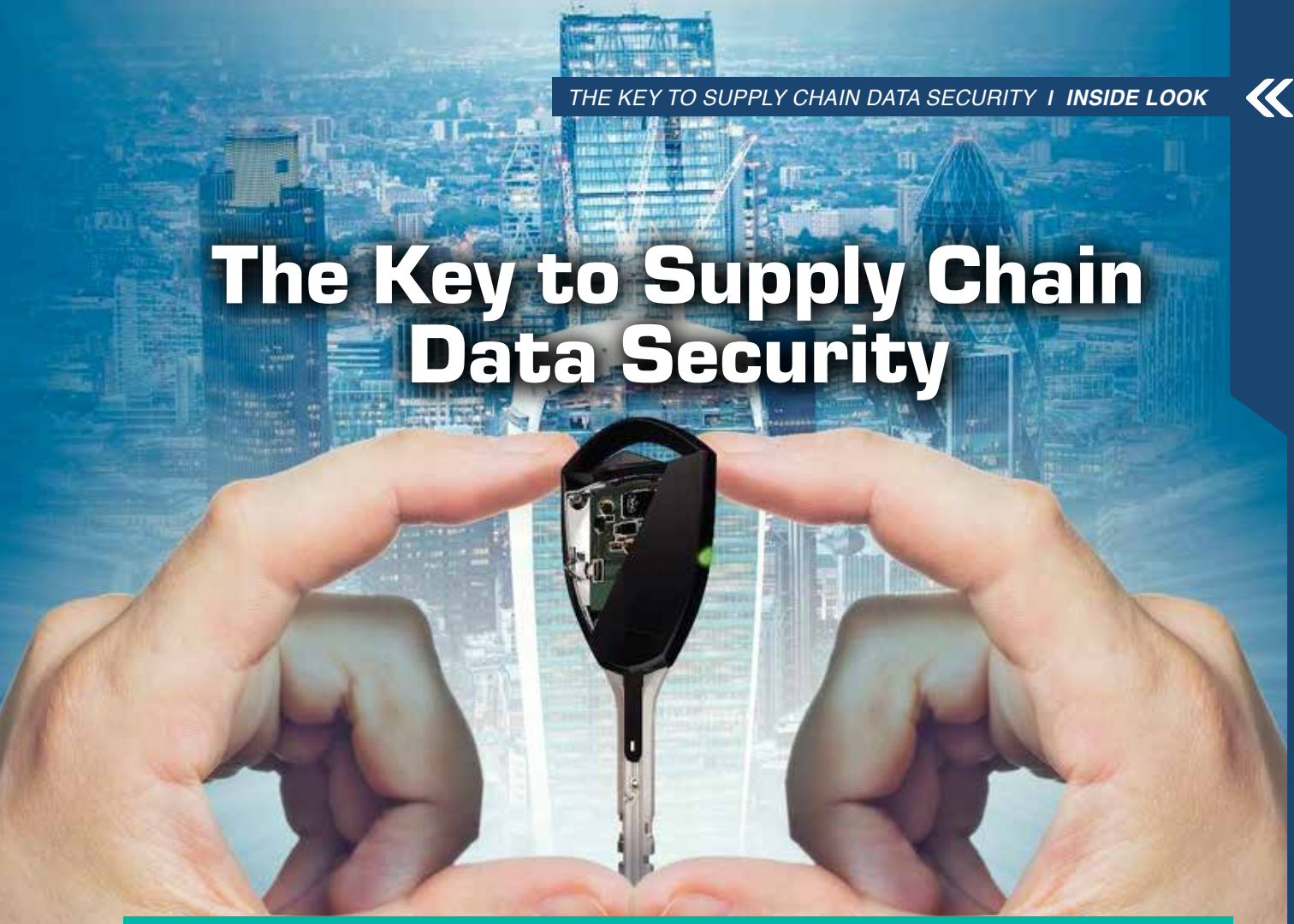
Techno-savvy and Trained

Intelligence-led policing is a concept that involves a number of factors coming together. It has been defined as "a business model and managerial philosophy where data analysis and crime intelligence are pivotal to an objective, decision-making framework that facilitates crime and problem reduction, disruption and prevention." Techno-savvy and trained police targets prolific and serious criminal offenders in an organised, thoughtful manner. With the growing amount of data in smart cities, techno-savvy policing would gather a wide variety of data from various sources for analysis and required actions.

- Defining and managing end-to-end process
- Building capacity in the right skills
- Cybercrime management
- Effective use of data

For more information, please visit: www.governancenow.com. SST

The Key to Supply Chain Data Security



Pip Courcoux, Sales and Product Manager - CLIQ Systems at Abloy UK, discusses the current issues around cyber security and explains why organisations must assess the resilience of their suppliers to minimise the risk of attack.

The landscape of security and access control has changed over the last decade, with the introduction of technology that allows for traceability and time management within mechanical keys.

This has meant the conversation has changed - Passkeys, Cryptographic keys, Encryption keys are all becoming more commonplace. By default, we've become obsessed with cyber security, and high-profile cases and examples of data theft and loss are rife.

Research shows that 93 percent of large organisations and 87 percent of small businesses experienced a security breach in 2013, with affected companies experiencing roughly 50 percent more breaches than in 2012 .

> *"Add to this the complex risks that cyber security poses and ensuring a safe supply chain environment can seem like an impossible task. How 'stable' are your suppliers, do you know where they get their products from, how safe and protected are their assets, and how robust are their own relationships with their suppliers?"*

Although keys provide access to critical assets, including servers that hold customer data and provide access to offices where customers' accounts are managed, we see many organisations that don't know how many keys they have in circulation, or where they are at any given time.

The Supply Chain

For organisations handling any kind of data, great importance must be placed on resilience within the supply chain. When considering exposure to risk, physical supply chain management presents a number of unique challenges.

Add to this the complex risks that cyber security poses and ensuring a safe supply chain environment can seem like an impossible task. How 'stable' are your suppliers, do you

know where they get their products from, how safe and protected are their assets, and how robust are their own relationships with their suppliers?

Mitigating risk can involve identifying dependencies and vulnerabilities that can impact upon supply chains. Increasing the visibility of these areas allows organisations to anticipate their impact and to plan for the contingencies.

Data Protection

When it comes to the security of your data, areas that need to be considered include:

- What information are you sharing within your supply chain?
- Where is the data located?
- What are your suppliers doing with that information?
- Are they reselling that data?
- Is there a data controller and processing agreement in place?
- Are they prepared for compliance to the General Data Protection Regulation (GDPR)? Enforcement date: 25th May 2018.
- How would you deal with a data breach?

The GDPR is a binding legislative act from the European Union for the protection of personal data. The Regulation tackles the inconsistent data protection laws currently operating throughout the EU's member states and facilitates the secure, free flow of data.

If an organisation fails to comply with the Regulation it could be fined up to 4 per cent of the company's global annual turnover – and could severely damage its reputation.

The Secure Option

To combat these risks, Abloy UK offers a high level of both physical protection, with its high-quality locking solutions, and data protection using only accredited software and infrastructure providers.

"The CLIQ® system enables the organisation to comprehensively track and audit who has access to which locations, when they had access and how often. Access can be granted only at the exact moment it is required, mitigating the risk associated with lost or stolen keys."

One example of this is PROTEC2 CLIQ®, an electronic key system where all the power is retained by the key or locks themselves. This means no wiring is required, whether the system uses door cylinders, cabinet locks or padlocks.

Users have secure access to the online management application from anywhere in the world and can change key access permissions, profiles, schedules and validity, even revoking their use virtually at the 'CLIQ' of a button.

CLIQ keys are validated daily, weekly or monthly keeping them continuously secure. Users are required to change their password every 3 months – but when was the last time you changed your keys?

The CLIQ® system enables the organisation to comprehensively track and audit who has access to which locations, when they had access and how often. Access can be granted only at the exact moment it is required, mitigating the risk associated with lost or stolen keys.

What's more, Abloy uses accredited software and infrastructure providers that provide enterprise level SaaS solutions, compliant with European and National standards for physically secure key systems.

Abloy also uses the latest techniques to secure its customers' data behind three factor authentications, standard 256-bit encryption, advanced encryption and industry standard SHA-2 SSL certificates.

So when it comes to data security within your supply chain don't leave anything to chance, mitigate the potential risks in advance and only use suppliers you can be sure will keep your data secure.

For more information, please visit: www.abloy.co.uk

THE FIRST CYBERSECURITY RULE WHEN IMPLEMENTING CARD-BASED SYSTEMS – ENCRYPT!

By **Scott Lindley**, President of Farpointe Data

Scott Lindley is a 25+ year veteran of the contactless card access control industry. He is president of Farpointe Data, the leading OEM for readers and credentials.

It used to be that the most important aspect of implementing an electronic access control system was the simple control of who went where when. Today, the requirements of these sophisticated systems goes beyond. Indeed, one of the security challenges frequently heard surrounds denying hackers, cyber-punks and associated bad actors from utilising the access system as a gateway to an organization's sensitive IT network.

As an RFID access card gets close to its reader, it begins to wirelessly transmit its binary code. If using 125KHz proximity, then the wireless protocol is typically Wiegand, an older technology that can no longer provide the security needed today. In a worst case scenario hackers could simply lift that fixed Wiegand clear text, retransmit it to the card reader, and, from there, physically enter the facility and thereby the network, allowing these characters free rein to target the IT system.

Many law enforcement agencies are starting to take action. For instance, the United States Federal Trade Commission (FTC) has been apprised of so many cyber attacks and the threat these hacks pose, that it is now holding companies responsible for not implementing good cybersecurity practices. As a result, data encryption is part of good practice and is, indeed, an opportunity for the security industry.

"Many law enforcement agencies are starting to take action. For instance, the United States Federal Trade Commission (FTC) has been apprised of so many cyber attacks and the threat these hacks pose, that it is now holding companies responsible for not implementing good cybersecurity practices. As a result, data encryption is part of good practice and is, indeed, an opportunity for the security industry."

3 Major Elements to Encryption

Authentication verifies that someone is who they say they are. Credentials are compared to those on file in a database. When matched, the user is granted access. ("Yes, badge #1234 is in our database. Go ahead.") Settings are defined by an administrator. For example, in a high security facility, the administrator may demand multifactor authentication, using a card plus PIN.

Integrity assures that digital information is uncorrupted and only accessed or modified by those authorised. ("Nobody has messed with this number.") Data must not be changed in transit or altered by an unauthorized person or program. If data gets corrupted, then redundancies restore the affected data to its original state.

Non-repudiation means that users cannot deny the authenticity of their signature on a document or the sending of a message that they originated. ("Nice try but we know that YOU did this.") A digital signature not only to ensures that a message or document has been electronically signed by the person but also ensures that a person cannot later deny they furnished it.

Here is How Encryption Works

Encryption consists of both an algorithm and a key. Once a number is encrypted, the system needs to have a key to decrypt the resultant ciphertext into its original form. There are two varieties of algorithms - private (symmetric) and public (asymmetric).

Private key encryption uses the same key for both encryption and decryption. Be aware - if the key is lost or intercepted, messages may be compromised. Public key infrastructure (PKI) uses two different but mathematically linked keys. One key is private and the other is public.

With PKI, either key can be used for encryption or decryption. When one key is used to encrypt, the other is used to decrypt. The public portion of the key is easily obtained for all users. However, only the receiving party has access to the decryption key allowing messages to be read. Systems may use private encryption to encrypt data transmissions but use public encryption to encrypt and exchange the secret key.

Using one or both these algorithms, access credential communications may be encrypted. Many modern cards support cryptography. Look for terms such as 3DES, AES (which the government uses to protect classified information), TEA and RSA .

Adding Encryption into an Access Control System

If concerned with hacking, consider more secure 13.56 MHz smart cards over 125 KHz proximity cards. Look for the term "Mifare," a technology from NXP Semiconductors. The newest Mifare standard, DESFire EV1, includes a cryptographic module on the card, adding an additional layer of encryption to the card/reader transaction. DESFire EV1 protection is especially important for customers wanting to use secure multi-application cards for access management, public transportation or closed-loop e-payment.

Another valuable option is Valid ID, an anti-tamper feature for contactless smartcard readers, cards and tags. Embedded, it adds yet an additional layer of authentication and integrity assurance to traditional Mifare smartcards. Valid ID helps verify that sensitive access data programmed to a card or tag is indeed genuine and not counterfeit.

Encrypted Cards and Readers Inhibit Hackers

Whether you need to guard against state sponsored terrorists or the neighborhood teen from hacking the electronic access control systems that you implement, security today starts with encryption. But, that's just a beginning. To take steps that will further hinder hackers, ask for your manufacturer's Cybersecurity Vulnerability Checklist.

For more information, please visit: www.farpointedata.com SST

Can Smart Cities Also Be Safer Cities?

By Hitachi Data Systems ©

A recent Safe Cities survey offers a revealing snapshot into the plans and progress of public safety initiatives across Asia Pacific and why integration is the key to success.

If Asia Pacific is on track to emerging as the world's most powerful economic region, its cities are also on their way to becoming some of the planet's smartest. A recent report predicted the number of smart cities worldwide to quadruple over the next ten years, with Asia Pacific expected to see the highest number of smart cities, reaching 32 by 2025, ahead of Europe and the Americas. But what does the term smart city actually mean?

Gartner defines a smart city as an urbanised area where multiple sectors cooperate to achieve sustain-able outcomes through the analysis of contextual, real-time information shared among sector-specific information and operational technology systems. Indeed, one of its most recent reports estimates that smart cities will account for more than 1.1 billion Internet of Things (IoT) items this year (2015), rising to 9.7 billion by 2020.

"Gartner defines a smart city as an urbanised area where multiple sectors cooperate to achieve sustain-able outcomes through the analysis of contextual, real-time information shared among sector-specific information and operational technology systems."

The question that needs to be answered is can smart cities be safer places for people to live and work? What role does the advancement of technology and IoT have to play in delivering public safety?

To find the answers, Hitachi Data Systems (HDS) conducted a survey of delegates at the Safe Cities Asia con-ference in Singapore in May 2015. The event was attended by city government representatives, agencies and key municipal leaders from Asia Pacific, who discussed public security and safety challenges. Over a quarter of the respondents had a technology background of some kind, with the rest ranging from city mayors and corporate CEOs to military, emergency services, and providers of infrastructure such as transportation and logistics.

In short, the survey provided the right sample base to identify the role that technology is currently playing and could play in the future, when it comes to delivering safer cities.

Serious Money Being Earmarked for Safer Cities

The results of the survey have been extremely revealing. Nearly 90% of respondents said that either they or their organisations had already been involved in a safety project. Moreover, 69% of respondents are planning to invest in public safety projects in their countries over the next two years. Nearly half (44%) of the respondents estimated that their countries would invest more than US$100 million in public safety projects during the next two years. Some 22% of them predicted that the investment would be higher, at between US$100-500 million, while nearly 14% anticipated spending over US$1 billion. This also raises another question: do governments know the best way to spend that money? When it comes to public safety, the answer might be no.

Are Governments Helping Or Hindering Public Safety Projects?

The majority of survey respondents (25%) felt that a lack of alignment between government agencies was actually holding back the implementation of public safety projects. One of the most popular reasons cited for sluggishness towards public safety is simply a lack of

government focus; an odd finding considering that public safety is one of the primary responsibilities of any government.

The main barrier to progress appears to be a failure to adopt an integrated approach to safety initiatives. The ideal solution would be to start by involving as many stakeholders as possible in the planning process, resulting in an execution that enables the implementation to play a wider role in making the city smarter and as safe as possible.

Technology Tackling Crime

When asked what areas needed to be addressed to realise the 'Smart City' goal, 22% of the responses had to do with physical development initiatives, including urban construction projects and enhancing or expanding transportation infrastructure. The advancement of Internet and IT capabilities was also high on the list, with a 17% response rate.

A staggering 95% of respondents rated the role of technology in ensuring public safety as Important or Very Important. The public safety technology that most plan to invest in over the next two years is surveillance, followed by big data analytics, and mobile and network technology. Indeed, the convergence of all three offers tremendous scope for improving both safety and security in modern cities.

The lessons learned from the big data revolution suggest that integration exploiting the capabilities of a variety of interconnected systems in real time offers far more value than standalone solutions in improving public safety.

Cities that fail to take a holistic, fully integrated approach to planning for the future are likely to remain stuck with the problems of the past.

One of these perennial problems is crime. However, some police forces are recognising that integrating new IT platforms with other city resources can have a dramatic impact in driving down crime rates and increasing public safety.

Urbanisation and transportation play important roles in monitoring and preventing crime by identifying criminal acts, or potential criminal acts, in advance. This can be done through advanced technology by combining and analysing data from a variety of sources, such as video cameras on trains, in department stores and scattered throughout the city, as well as other data on social platforms such as Twitter. Powerful analytics tools digest the totality of the information to extract key insights that can identify 5% crime hot spots.

This use of technology is an attractive prospect for the public sector because it doesn't require the usual rip-and- replacement cycle that most IT implementations call for. Rather, by taking a holistic approach, supported by appropriate enabling technology, a city can leverage its existing infrastructure and resources to create innovative and effective public safety solutions.

Conclusion

The ultimate goal for any city smart or otherwise is to create an environment where people can live without worrying about safety.

The secret to creating smarter and safer cities is not to work a little harder in a few specific areas. The real solution is to stop looking at each of these safe city components in isolation. To be truly effective, a municipality should view and manage all of the various parts together holistically. This allows each piece of the smart city puzzle to support the others. Moreover, by taking an integrated approach and employing more comprehensive analytics, the potential benefits multiply tremendously.

For more information, please visit: www.HDS.com SST

AN INTERVIEW WITH

JIM TREINEN

VP OF THREAT, CARBON BLACK

What are the most alarming cyber security threats governments and organisations are facing today?

The most alarming cyber security threat faced by governments and organisations is the increased prevalence of non-malware attacks.

During the past six months, Carbon Black's Threat Analysis Unit (TAU) analysed more than 1,000 ransomware samples and found that attackers are looking to make quick, easy money with unsophisticated malware combined with sophisticated delivery methods. The majority of today's ransomware aims to target the largest vulnerable population possible.

In addition, 99% of the ransomware targets Microsoft products and some variations are beginning to launch fileless (or non-malware) attacks. Non-malware attacks are so dangerous because they work. These attacks leverage on trusted, native operating system tools such as PowerShell or exploit running applications, such as web browsers and Office applications, to conduct their malicious behavior. The nature of these attacks allows hackers to gain control of computers without downloading any malicious files, which means that they can bypass detection by traditional antivirus (AV) software, which was designed to stop malicious files only.

What is perhaps more alarming is the general unpreparedness of worldwide businesses to handle these attacks as demonstrated by the recent WannaCry and NotPetya attacks.

What is Threat Hunting and how can organisations leverage this for their cyber security strategy?

Threat hunting is the active pursuit of abnormal activity on servers and endpoints that may be signs of compromise. The concept isn't new, but many organisations are just getting started with threat hunting. The common approach to intrusions is to respond after getting an alert. This is a passive approach as attackers could be inside your systems for months before you know it. Rather than wait for alerts, threat hunters proactively look for anomalies.

Threat hunting needs to be instilled as a process that security teams make and schedule time for. To do this effectively, you need tools that give you granular visibility into every endpoint and server — things like processes that are launched, files that are opened, and network communications that take place. Tools such as Cb Response are tailor made for effective threat hunting across an enterprise.

Threat hunting is becoming a part of infosec table stakes - the essential tools and practices required by all organisations. Threat hunting will soon be a part of the due care for information protection expected by customers, regulators, and the legal system.

Why and how should businesses adopt an offensive stance towards cyber security?

Cyber criminals are constantly evolving their methods of attack and organizations should evolve their technology to tackle the latest threats. This means moving away from legacy AV and adopting a new line of defence that has been specifically developed to address sophisticated threats.

The new model of prevention, known as Streaming Prevention, is a radically different approach to cybersecurity. Traditional defences like legacy AV and

> *"By using underground markets and the dark web, Ransomware-as-a-Service provides an adversary with no technical experience the ability to easily sponsor a ransomware campaign with available funds."*

machine-learning AV are designed to only identify threats at a single point in time (i.e. when a malicious file is downloaded), making them completely blind to non-malware attacks. Streaming Prevention flips the coin by adopting an offensive stance – it monitors the activity of applications and services, including communications between processes, inbound and outbound network traffic, unauthorized requests to run applications, and changes to credentials or permission levels. By analysing these relationships and clustering events, Streaming Prevention can identify abnormal behaviour, which can be tagged, flagged and automatically shut down before the attackers can achieve their goals.

Please share with us on your outlook for cyber security in the rest of 2017 and the year ahead as well. Can we expect more ransomware attacks?

Carbon Black TAU expects a rising-tide evolution of ransomware in the coming months as attacks attempt to further extort money from unprepared businesses and consumers. Some other key predictions include –

- Ransomware will become more targeted by looking for certain file types and targeting specific companies such as legal, healthcare, and tax preparers rather than "spray and pray" attacks we largely see now.
- By using underground markets and the dark web, Ransomware-as-a-Service provides an adversary with no technical experience the ability to easily sponsor a ransomware campaign with available funds.
- Ransomware will emerge as a secondary method when initial forms of attack fail. Adversaries that rely upon more crafted and targeted attacks may use ransomware as an attack of last resort.
- Ransomware will increasingly leverage social media to spread either intentionally or unintentionally. Similar to malware such as Koobface, maliciously shared content on sites such as Facebook could lead victims to click enticing links.

In your opinion, is cyber vigilance at an optimal level in the Asia Pacific region? What can be done to improve the situation and educate organisations on the importance of cyber readiness?

According to IDC, 84% of organizations across APJ are operating with less-than-ideal IT security strategies in place, while a study conducted by the Australian Strategic Policy Institute (ASPI) found that the cybercrime maturity across the region is highly varied. Given that cybercrimes are not confined by geographical boundaries, cybercriminals only need to identify a single point of failure and use it to launch attacks into the networks of more advanced countries.

Thanks to recent headlines, cybersecurity is in the spotlight. As a result, we'll hopefully see governments and business leaders make a concerted effort to prioritise defense against advanced cyberattacks. The good news is that many organisations see this problem and are allocating adequate budget. The bad news is that too many organisations are under-educated and simply 'checking the box' by implementing the bare minimum. Others continue to attempt to tackle pertinent threats, such as ransomware, with the same ineffective technology. This is a recipe for a major recovery bill down the road when the inevitable attack does occur.

What are some basic steps that organisations can implement in order to protect their data from hackers?

Develop a Strategy

A multi-layered security infrastructure is essential in order to confront the adversaries from every angle.

Part of your strategy should include cost management – investing in the right mix of cybersecurity solutions for your organisation. Currently, organizations are still investing heavily in traditional AV and network security. However, incumbent AV providers regularly miss critical malware threats, as reported by Gartner in its 2016 Magic Quadrant for Endpoint Protection Platforms. To close this critical security gap, organizations can look to next-generation technologies like Streaming Prevention.

Maintain Real-Time Inventory and Actionable Intelligence

Millions of attack happen every day. This is why real-time surveillance is now critical for identifying and stopping attacks before they accomplish any real damage. This can be easily addressed with a solution that can continuously scan, monitor and collect data from an organisation's endpoints, reducing detection and response time significantly.

By collecting detailed and actionable information on these security threats at a granular level, organisations can also attain a deeper level of insights on why and how a breach occurred, with the end goal of making it exponentially more difficult and expensive for attackers to do their work.

Conduct Regular Audits

Once a robust security infrastructure is in place, regular audits of security measures, especially connections commonly used as gateways for attacks should be carried out in order to access and re-evaluate if an update is needed.

Cybercriminals are constantly innovating and advancing their tactics of attacks. It would be foolhardy to assume that the technology of yesteryears is still effective against today's threats.

Educate Employees

When it comes to cybersecurity, the human is often the weakest link. Ensuring that all employees are clear on their role in data security and raising awareness on the types of threats goes a long way in closing any possible gaps in your cybersecurity infrastructure.

What challenges will cyber security professionals face in the years ahead, in light of the digitalisation of society (IoT) and data being moved to the cloud at a rapid pace?

The threats and vulnerabilities are similar. The challenge with IoT is with the manufacturers who design the technology. Very often, the devices are black boxes that don't allow you to fit anything - security solutions for example - after it has been manufactured. The IoT security problem must be addressed on the manufacturer level – devices need to incorporate security by design. Cheap IoT equipment manufacturers often cut costs by minimising the maintenance of these products. As such, enterprises need to be discerning of how enterprise-ready these IoT devices are before investing in them.

With the recent ransomware attacks, cloud providers have stepped up tremendou sly on the security front by using the latest technologies. Although this is an advantage for companies looking to migrate to the cloud, cybersecurity is never fail proof. Business leaders must understand that they can never be too safe when it comes to cyber threats. Implementing a cybersecurity strategy in the cloud is imperative and the cloud providers will not be held responsible for data outages and loss. SST

"Very often, the devices are black boxes that don't allow you to fit anything - security solutions for example - after it has been manufactured. The IoT security problem must be addressed on the manufacturer level – devices need to incorporate security by design. Cheap IoT equipment manufacturers often cut costs by minimising the maintenance of these products. As such, enterprises need to be discerning of how enterprise-ready these IoT devices are before investing in them."

AN INTERVIEW WITH

BOYE VANELL

REGIONAL DIRECTOR, ASIA, BAE SYSTEMS APPLIED INTELLIGENCE

Could you please tell us more about your collaboration with NTU in developing next-generation cyber security solutions? What solutions do you have in store to address the increasing amount of ransomware attacks and hacking incidents?

Our research collaboration with NTU aims to uncover better methods for predicting and mitigating cyber attacks before they happen. This is being researched through fusing large data sets of threat intelligence information about known threat actors to understand their tactics, techniques and procedures (TTPs), and build these into machine-readable Threat Operating Models (TOMs). The intention is for TOMs to be measured against the characteristics of a company or government's operating environment, such as the types of applications, software and hardware used by them. It then identifies environments that present a higher risk of matching a known threat actor's motives and TTPs, therefore giving them pre-warning of a likely attack.

We work to incorporate TOMs into our cyber detection and threat analytics platforms to give Security Operating Centers (SOCs) early warning, especially when their operating environments start to match the ideal conditions of threat actors operating in their region. TOMs could also be tailored for common strains of ransomware to alert organisations to when they are at a greater risk of an outbreak – for example, when a critical patch in preventing a damaging strain of ransomware has not been widely applied.

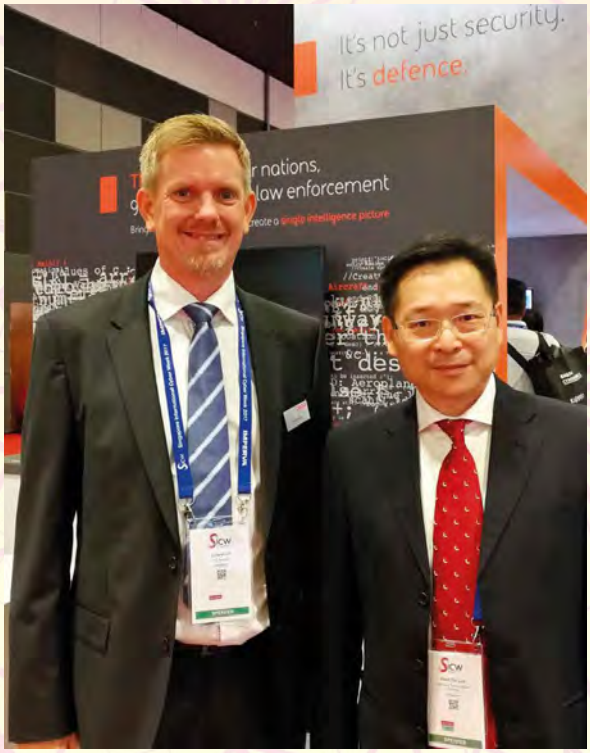
How can Artificial Intelligence (AI), Natural Language Processing (NLP) and text analytics assist in developing a safety net to protect organisations against hacking incidents?

Threat intelligence information is usually in human-readable formats, such as English, Russian, and Chinese. As most material is unreadable without human or machine translation, cyber analysts will typically be conversant in one or two languages. However, the volume of threat intelligence material being produced may exceed what an analyst can read and act on. By using Natural Language Processing (NLP) technologies, a machine can automatically parse and summarize threat intelligence information. The derived information can be used to automatically assess the threats that a given organisation may face, or to auto-generate new detection signatures to deploy on firewalls.

One of the areas of research we're working with NTU on is a way to derive information from images. While reading and understanding text within images – such as photos – is something we take for granted, it poses some difficultly for machines. Artificial Intelligence methods that are similar to the workings of the brain are being researched to automatically recognise and extract text from images. This text can then be indexed, searched and parsed or otherwise post-processed. This capability means that the automatic processing of intelligence reports can go beyond text and additionally bring in information from images, such as screenshots.

What roles do a nation's laws and policies play in influencing the cyber security landscape?

As was recently discussed during CSA's request for industry feedback on the new Singapore cyber security legislation due in 2018, a nation's laws and policies can



> *"We work to incorporate Threat Operating Models (TOMs) into our cyber detection and threat analytics platforms to give Security Operating Centers (SOCs) early warning, especially when their operating environments start to match the ideal conditions of threat actors operating in their region."*

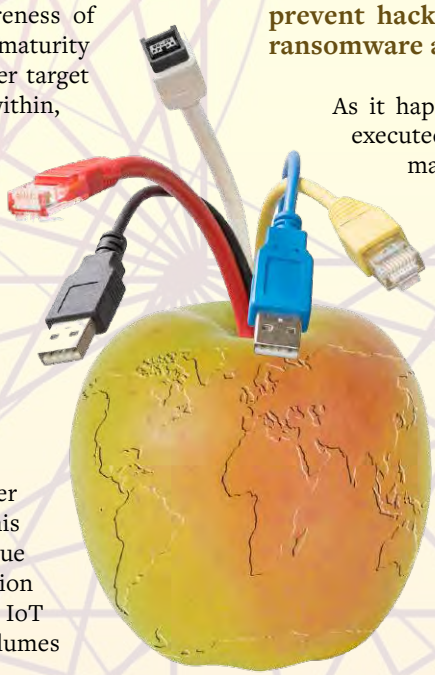
have a profound impact on the local cyber security landscape. Countries with a vibrant cyber security landscape and empowered government agencies anecdotally demonstrate higher levels of cyber security maturity across the general populace. This vibrancy and empowerment is often directly related to creating legislation that encourages cyber security start-ups to flourish, and provides the authority for agencies to act on cyber security incidents, while broadly increasing security awareness of its citizens. The higher level of maturity across a country presents a harder target for cyber threats to develop within, and enhances the economic and skills benefits when growing a high-tech industry.

What are some of the cyber security problems that organisations in the Singapore and the Asia Pacific region face? How can we address these issues via innovative solutions?

Singapore is an especially hyper connected country and this trajectory is set to continue with the growth of Smart Nation and the integration of more IoT devices. In addition, the volumes of personal data being stored by more and more organisations present attractive targets for cyber criminals and privacy concerns for citizens. This risk of the interconnectedness and centralisation of data is compounded by the limited cyber security skills available in the country.

Defensive solutions need to focus on doing more with less – that is, creating innovative solutions that enable the limited talent available to make the most effective use of their time, through better situational awareness of what is happening in their networks, and through the automation of repetitive tasks.

In this era of IoT where many countries are aspiring to become full-fledged SMART nations, what basic measures can be implemented to prevent hacking incidents or safeguard from ransomware attacks?



As it happens, a lot of the basic measures are executed poorly, which often contribute to major cyber security incidents. Simple concepts like regularly patching systems and improving general security awareness across the population would prevent a majority of incidents happening. For example, the patch that prevents the WannaCry malware from spreading was released months before the major outbreak.

As we move into the era of IoT, these concepts will not change. IoT vendors need to factor security in from the point of product development, to reduce the need for ongoing patches and configuration

updates. Similarly, governments need to legislate and accredit solutions that have the necessary security measures built in from the start, to discourage the spread of cheap and insecure devices.

Why is the collaboration between the private and public sector as well as academia integral to ensuring cyber safety?

Each organisation brings different strengths and weaknesses to the problem. Governments have the authority and budgetary power to improve security maturity, but are generally the slowest to make progress. Private companies are more agile and can move faster, but will only solve a problem when it makes commercial sense. Academia are less restrained by the profit driven commercial rhythms and benefit greatly from Government R&D funding, allowing them to spend more time researching innovative and long-term solutions to problems.
By combining the best elements of each sector, a vibrant industry can grow and problems can be solved with long-term thinking, contextualised for the country.

What can be done to increase cyber readiness and vigilance in Singapore? What are some basic steps that organisations can follow when confronted with Ransomware or other incidents in which their data is compromised?

Organisations need to ensure they have mastered the basics first. The cyber security industry is still immature, and it can be a trap for organisations to get drawn into thinking that the flavour-of-the-month technology will solve all of their problems. There is no one solution to becoming 'cyber secure'. Applying security patches, improving security awareness for staff – such as identifying phishing emails – and having capable incident response staff will mitigate much of the damage caused by ransomware and other security incidents. SST

"The cyber security industry is still immature, and it can be a trap for organisations to get drawn into thinking that the flavour-of-the-month technology will solve all of their problems. There is no one solution to becoming 'cyber secure'."

Dahua's New Alarm Adds Safety to Home Living

Homes are supposed to be safe, but unfortunately, they are not some times. That is a fact we have been reminded by all those shockingly tragic news from time to time. People couldn't help but wonder: Why do these tragedies have to happen? Is there anything that can be done to prevent them from happening?

Now these questions have been answered by Dahua's new alarm kits, DHI-ART-ARC5402A-GW-06-A35 and DHI-ART-ARC5402A-GW-10-A35-C35, which are capable of providing solid protection to all families. The following are some of their feature highlights.

Dahua Home Wireless Alarm Kit

Airfly Communication Technology

Based on radio frequency of 433/868/915MHz, Airfly is a private wireless communication technology of Dahua, a two-way communication that is safer than one-way communication, offering 128-bit AES fully encrypted wireless communication with dynamic key.

4.3 inch TFT Screen

Dahua's 4.3 inch TFT screen (480*272 resolution), a design for convenient to install and easy to control.

ARC5402A-GW Video Alarm Control Panel

ARC5402A-GW, the video alarm control panel that is the "brain" to Dahua's alarm system, boasts functions such as alarm information collection, alarm output and linkage control, PSTN alarm reporting, alarm SMS, audio message, IPC surveillance, video recording and playback.

Alarm Panel Features

Besides what's aforementioned, the whole system supports up to 32 wireless zones, 2 wired zones, 8 remote controls, 4 wireless sirens, 1 wired siren and 1 wired PGM output; Wi-Fi (IEEE 802.11) , PSTN, GSM and TCP/IP RFID reader (that allows you to arm or disarm without password) and the backup battery (3.7V/1900mAh, Li-ion).

Put together, Dahua's alarm system works in a stable and low energy consuming manner, sending you any signs of threats in time and providing you with full range of options to respond.

Application Areas

Shops

A shop is a place of many goods and people, which means there is a lot at stake. Dahua's alarm system can push alarm message on your smart phone. Also you can access video through App—DMSS.

Villas

Villa stands on its own, which means if there is any emergency in the villa, outsiders usually can't come to help in time. In addition, villa contains huge space, often disproportionate to the number of people living in. You need wireless door/window contacts and PIR to detect intrusion and threats from outside.

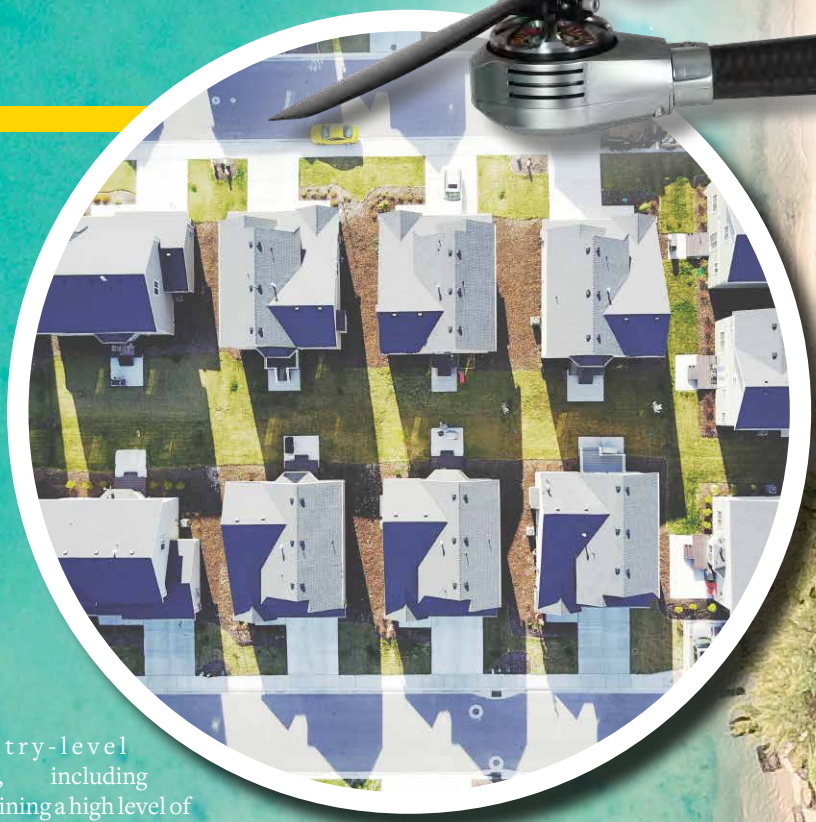
Apartments

During a time when no one is in the apartment, such as family vacation or weekdays, if a burglar broke into the door, the door contact will be triggered by the movement and send an alarm signal to the panel, which will then inform the host about the alarm through app-DMSS or short message. Also, when a burglar moves in the house and enters into the detection area of the PIR (Passive Infrared) detector, alarm will be triggered, too.

Dahua's new alarm system is designed to enhance home safety by alerting home owners of abnormal events and providing visual verification means. Airfly encrypted 2-way wireless communication technology allows this system to be conveniently installed in any place. As a result, more homes could be protected by alarm systems. With a mission of "Enabling a Safer Society and Smarter Living", Dahua will continue to focus on "Innovation, Quality, and Service", to serve partners and customers around the world.

For more information, please visit:
www.dahuasecurity.com SST

Dahua Drone X820 Guarantees Public Safety



As one classical Chinese poem goes, "The swallows once in mansions of the great now fly to ordinary peoples' homes". UAV (Unmanned Aviation Vehicle),. more commonly known as drones, are just like those swallows: once only found in military applications and war films, are now widely used in daily life. Military UAVs now are vastly outnumbered by civilian UAVs, whose use is expanding to commercial, scientific and even recreational realms. What distinguishes a Dahua Drone from other Civilian UAVs is the mission it is born with: to guarantee safety from above.

What Is an Industry-Level Drone?

There are in fact two levels of drones, consumer-level and industry-level. Dahua Drones belong to the latter.

Consumer-level drones are mainly designed for use in aerial photography and personal shooting/sharing for entertainment. Naturally they are pretty straightforward to operate and can take easily editable images/videos, often with automatic beautification and other entertainment functions.

This contrasts with industry-level drones that are built for serious public security mission such as power tower inspection, forest fire detection, public event management, security supervision over long bridges, detection aid for police forces, inspection of high speed traffic and other illegal incidents. It means that a very different set of functions are required for industry-level drones, including maintaining a high level of stability and safety, intelligent control, adaptability to different applications and environment, long distance mapping abilities, carrying capacity, and long battery life.

Dahua Drone X820

The current industry-level drones boast the capacity to transmit images at up to 10km, and with access to multi-VMS platforms, they can put real-time audio and video streaming on the screen of a control center, thus providing information for police or security companies to solve the problem on site, such as directing crowds for evacuation via the correct route or sending out a medical team to the location where it is needed.

Application Scenarios

Dahua Drones are easy to operate and use in situations such as the following scenarios.

Power Tower Inspections

Often located in mountainous areas, power towers are hard and risky to reach. Dahua Drones can enhance the efficiency while making it less labour-intensive. Benefitting from x30 optical zooming ability, Dahua Drones can capture HD images at a long distance, thus avoiding the accidents that ordinary drones have encountered as a result of electromagnetic interference from high-voltage power grids and visual mistakes by people operating from afar. The thermal camera they carry can accurately locate abnormally hot spots in cables and insulation terminals, thus preventing accidents from occurring.

Forest Fire Detection and Control

Via the thermal camera it carries, Dahua Drones can detect suspicious hot spots invisible to naked eyes. At a height of 1500m, a Dahua Drone covers an area of 5km², doing the inspection work of dozens of people in just one flight.

When there is a fire, Dahua Drones can fly to the site against high temperatures and strong winds, transmitting relevant data to ground teams, so that they can make the right move using this information. Once the fire has been extinguished, Dahua Drone's overhead inspection can prevent a second fire. In this sense, Dahua Drone is one of the best aids to help fire fighters.

Detection for Police

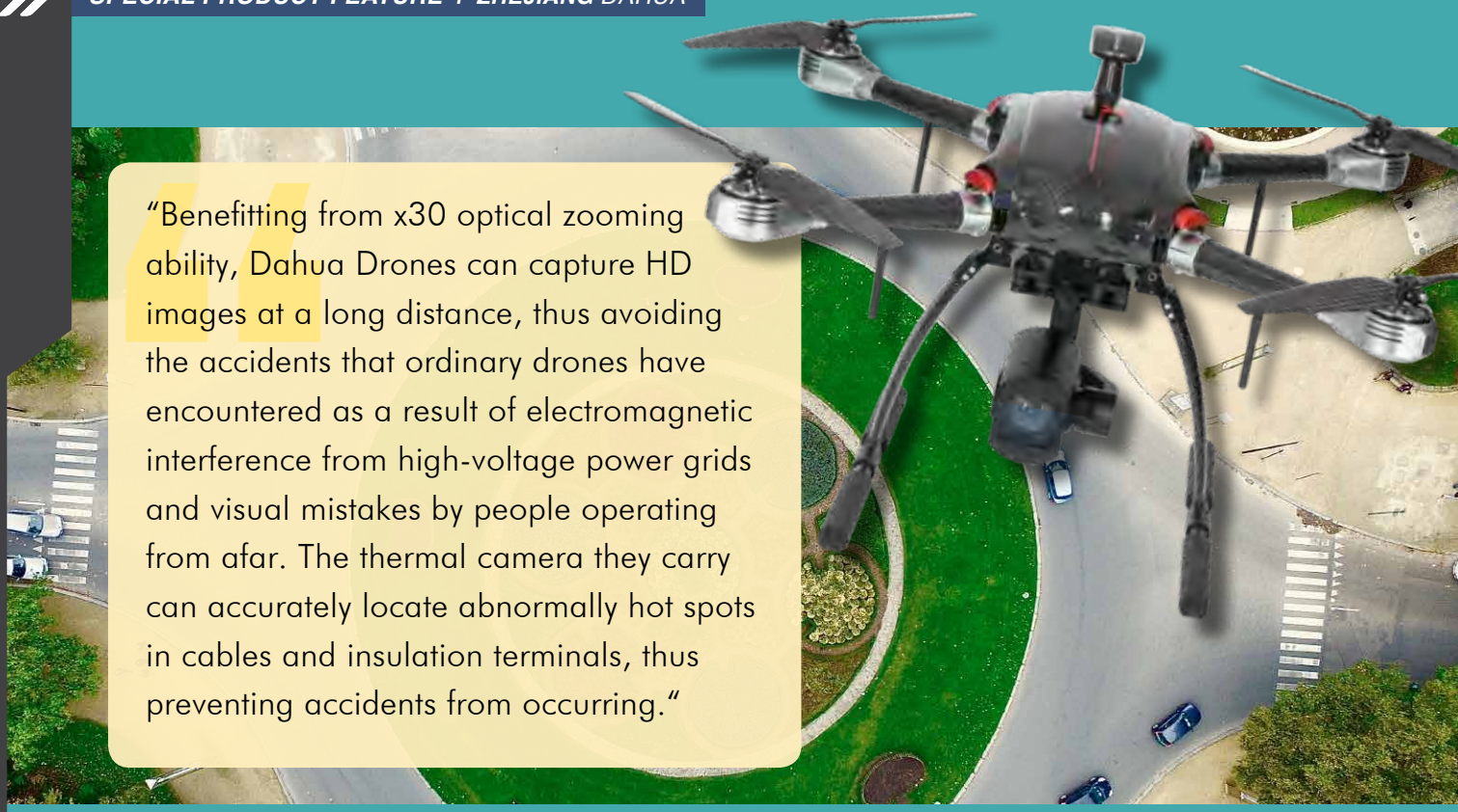
Arriving swiftly and secretly at crime scenes, Dahua Drones record real-time visual information about locations, traffic and personnel using its multifunctional camera, which is capable of optical zooming x30 (allowing the drone to work from a long distance where it won't be noticed by criminals); thermal imaging (allowing the drone to work at night) and automatic recognition of faces or wanted cars.

Using wireless transmission the information collected is accessible to all mainstream VMS platforms. In short, it is a very powerful assistant for the police.

Public Security Management

At public events like concerts, sports meetings and marathons, a Dahua Drone can provide special security surveillance from up high

"Arriving swiftly and secretly at crime scenes, Dahua Drones record real-time visual information about locations, traffic and personnel using its multifunctional camera, which is capable of optical zooming x30 (allowing the drone to work from a long distance where it won't be noticed by criminals); thermal imaging (allowing the drone to work at night) and automatic recognition of faces or wanted cars."



"Benefitting from x30 optical zooming ability, Dahua Drones can capture HD images at a long distance, thus avoiding the accidents that ordinary drones have encountered as a result of electromagnetic interference from high-voltage power grids and visual mistakes by people operating from afar. The thermal camera they carry can accurately locate abnormally hot spots in cables and insulation terminals, thus preventing accidents from occurring."

because of its multiple flying modes (circling around and tracking down the target), while its powerful camera can capture the whole picture as well as specific details and whilst benefiting from its long 38 minute battery life.

The beauty of a Dahua Drone lies not only in its ability to work from afar but also its safety whilst flying. Having undergone all sorts of extreme tests, this means when in use, a Dahua Drone will not disturb the crowd below at all.

Take New York City Marathon for example. There are thousands of participants and spectators spreading over a range of over 26 miles. It is quite a challenge to set up an effective surveillance system for such a 1 day event. Dahua drone can be very useful for such scenario. If properly deployed, 8 sets of model 820 drones can deliver very good coverage for the entire marathon. Each drone could take care of 6 km range by patrolling back and forth, staying still a few minutes at each of the 6 patrol points 1 km apart to have a good look at the situation under. These drones will be flying at 100m above ground to produce sufficient clarity to effectively identify mass casualty incidents such as stampedes or a traffic accident.

Obviously similar deployment of drones can also be applied to scenarios such as music festivals, open-air concerts and important political rallies, which will not only help security companies to work more efficiently but also provide evidence if illegal incidents occur.

Inspection of Bridges

The construction of massive bridges requires inspection, which usually takes lots of boats, equipment and experienced staff. Dahua Drones can greatly simplify the process and reduce the cost of money and time.

Dahua Drones can fly all around the bridge, checking the erosion, damage and other damages, while keeping a numbered record for experts to analyse afterwards.

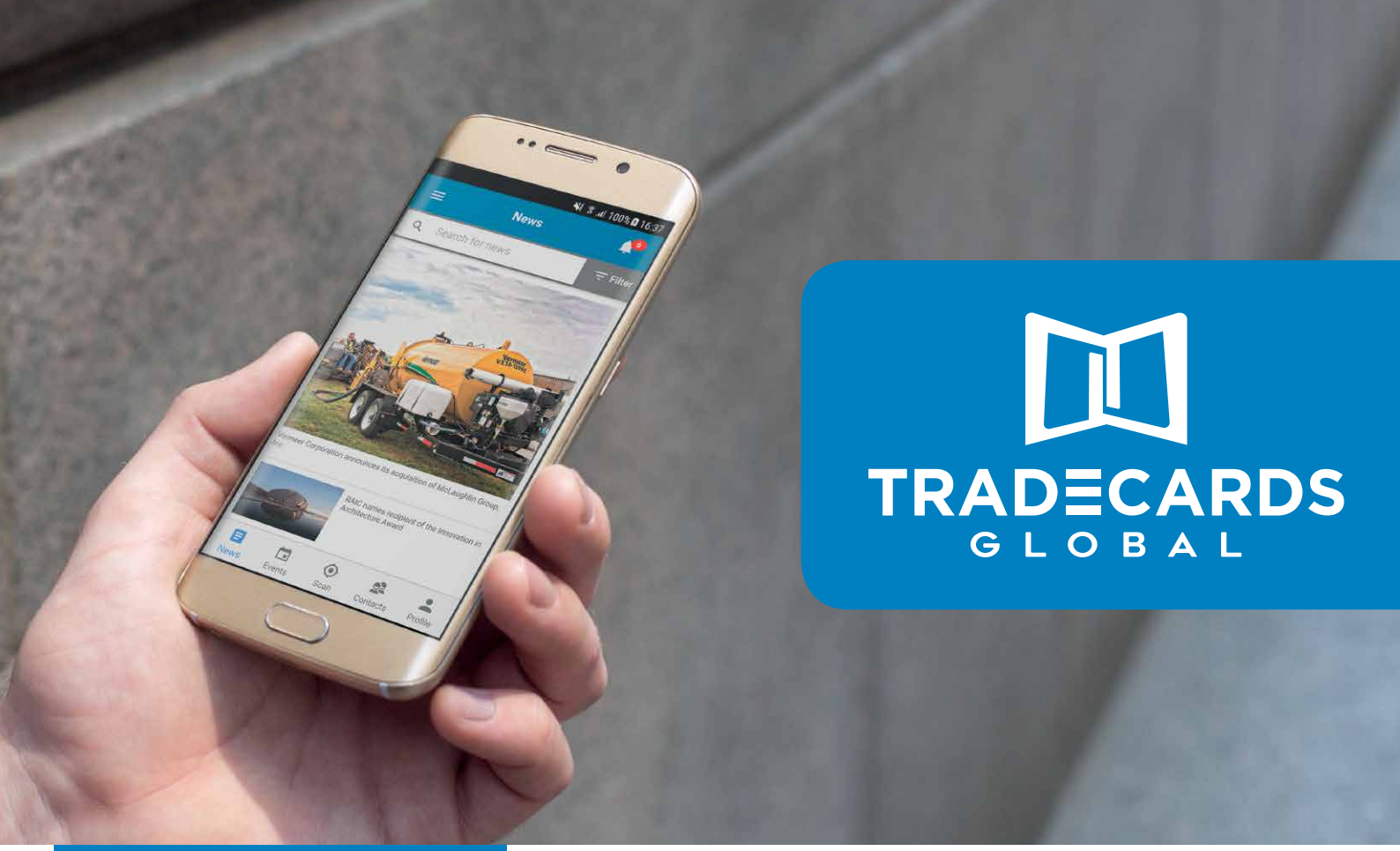
It's worth adding that Dahua Drones boast an outstanding ability to resist the wind (up to Windspeed 7.0), and are fully capable of maintaining highly accurate suspension over the river and providing stable visual information.

Inspection of High Speed Traffic

In daily patrols, when suddenly encountering the illegal behaviour of a driver, Dahua Drones can capture the HD image of it from afar and keep the record as evidence. Information about the car, the license plate and the driver will be immediately identified after the video is simultaneously transmitted to the back-end. In another scenario, if there is a traffic jam on a highway and nobody knows what is happening, Dahua Drone can provide real time and first hand images/video for related department to decide.

In conclusion, Dahua Drones can play a key role in various public security scenarios. Dahua has caught the latest technology trend and adapted to enable a Safer Society and Smarter Living. This is the future that Dahua Drones are helping us towards.

For more information, please visit www.dahuasecurity.com SST



TRADECARDS GLOBAL

TRADECARDS Global is a digital social platform for networking amongst trade professionals in various B2B industries.

Now serving B2B industries for:

Architecture
Audio Visual
Broadcast
Construction
InfoComm
Mining
Real Estate & Property
Safety & Security

VISIT OUR WEBSITE AT
www.tradecardsglobal.com

FEATURES

Scan for contacts
Scan and add nearby business contacts onsite during networking or trade events

Organisational listing
Create your organisational listing to target audience within specific industries

Industry news
Access to the latest news and updates from various industries

GET IT ON Google Play

COMING SOON

Download the App Store

ACTi Q950

By: Acti | www.acti.com

This 7-in-1 Door Station features intercom for two-way audio communication, 6MP fisheye camera for visual validation, RFID sensor for automated access control,door contact and lock control for remote management,touch-sensitive doorbell button with optional face identification for additional layer of security and passive IR for proximity detection.

Key Features include intercom with Two-way audio communication and a Touch Button with touch-sensitive button can be tapped over and over again without wearing down like conventional physical buttons. 180° High Resolution View to visually validate the visitor's identity through the eyes of a fisheye lens. The exceptional video clarity is achieved by a sensor with 6 megapixels, the highest resolution in the industry. Other features include Clear Video in Complicated Light , RFID Sensor, Face Identification, Environmental Casing and Shock Detection.

IP POE Access Door Reader

By: XID | www.xid-tech.com

The POE Access Door Reader proves flexibility in credential model choices with multi RF card as 13.56MHz ISO14443A/B, Mifare®Classic S50/S70, Mifare® plus, Mifare Desfire® EV1, ISO15693, Sony Felica, EM125KHz.

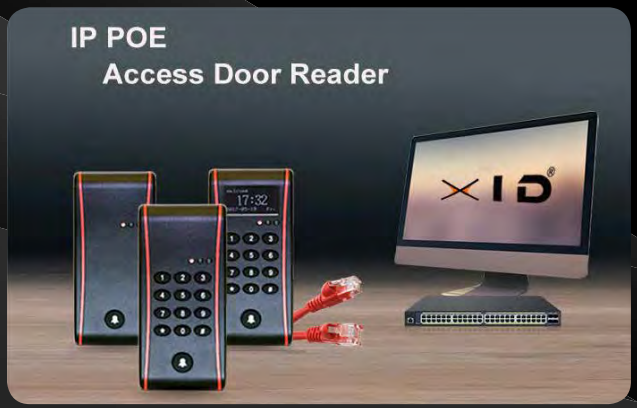
Along with popular and SMART mobile phone access control solution in ISO/IEC18092 NFC, NXP original RF chip and 128bit AES,DES/3DES high encryption algorithm integration to avoid cloning and copy is also included.

The reader comprises of reading distance can up to 5~10cm (Depending on antenna) and diversified communication interface as RS232/RS485, TCP/IP and Weigand 26,34,40,42,50,56,58 universal Wiegand protocol output to flexibly integrate into any other third party systemWide voltage range design 9~24V for different system. There are various kinds of working modes as multi RFID cards, NFC smart phone and PIN.

POE(IEEE 802.3af) eliminates the need for large numbers of AC power supplies or the installation of new AC outlets at the remote modes and OLED display to realise wide angle, high contrast, quick response and wide color field display(visible in sunlight).

Users can enjoy firmware online upgrade to obtain latest system during the first time and APB (anti-passing back) function to avoid illegal following. The appearance design consists of the XID patent and is IP65 waterproof for indoor and outdoor usage.

Other features include Strong environmental adaptability -20 ~60 , authorised certification CE, Rohs, CCC, FCC and one year warranty time (not being damaged by any man-made factors).



IPCAM-WICI HD Wi-Fi® Indoor Video Camera

By: Honeywell | www.security.honeywell.com

The next generation of Honeywell Total Connect Video now includes two high-definition indoor cameras and one outdoor camera which allows end-users to capture crisp, clear video of events and activities from Honeywell Total Connect 2.0.

For indoor applications, new IPCAM-WIC1 offers up to 720p at 30 frames per second, with a wide angle view of up to two detection areas and captures up to 1080p at 30 frames per second and offers a wide angle view of up to four detection zones.

For outdoor use, IPCAM-WOC1 offers up to 1080p at 30 frames per second, wide angle view and up to four detection zones. With simple QR code-based setup, new camera line is faster and easier to install.

Honeywell Total Connect Video increases overall number of installs per day and is feature-rich, next generation camera package will enhance customer offering and enables users to compete more effectively and grow RMR.

Features include integration so it works with proven winner Honeywell Total Connect Remote Services and Lyric™ security and home control systems. Fast and easy installation QR code installation with compact hardware and multiple mounting options– ceiling or tabletop with

Expansive memory ie, Cloud Video Storage - 7 day or 30 day per 8 cameras, per location, per month and local Storage - up to 64 GB, 8 GB included. (Provides backup storage in the event of Internet outage.). Stay connected with enhanced Wi-Fi® connectivity and range with 802.11n.

GSR-360

By: Infinti Optics | www.infinitioptics.com

Ground Surveillance Radar uses latest generation pulse-Doppler solid state technology to provide complete 360° coverage for 24/7 day night situational awareness with up to 1200km² of vehicle detection and 300km² of human detection. Military-grade commercially available high-performance ground and marine surveillance radar with small lightweight rugged IP67 ideal for tower, mast, shipboard, and mobile deployment.

Applications include force protection military compound, rapid deployment man portable and mast critical infrastructure protection, perimeter security and oil and gas pipelines along with border surveillance and homeland securit for wide area situational awareness and threat detection.

O-R3 Aerial Outdoor Security Robot

By: otsaw | www.otsaw.com

Powered by OTSAW AI, a confluence of computer vision, 3D SLAM and advanced machine learning technology, This outdoor security robot is able to patrol the streets and avoid dynamic obstacles with self-charge when its energy is running out.

Varied Cameras comprise of Specialised cameras enables O-R3 to capture and access wide range of information with thermal imaging, facial and license plate recognition and stereo photography. Highly Precise Sensors are equipped with numerous 3D and 2D laser scanners, IMU and ultrasonic sensors, GPS and long range data transmitters that collects most granular of data.

Features include Augmented Intelligence with Sensor fusion technology, ground-aerial collaborative surveillance, incoming real-time alerts, human-robot collaboration, with manual takeover and 360 degree surveillance scope, 24/7 patrol and protection and consistent productivity.

Somfy One

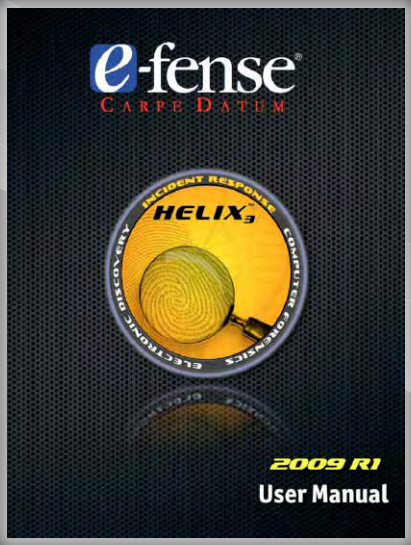
By: Somfy Protect | www.protect.somfy.co.uk

This all-In-One security solution including a siren, camera and motion sensor with HD camera with night vision that has built-in 90+dB siren with alerts sent immediately upon detection that are compatible with alarm accessories.

Powerful, Intruder-Deterrent Siren so that when intrusion is detected in the home, 90+ dB siren goes off automatically to scare off intruder. Trigger the siren manually with a simple click from smart phone. Photo and Video Proof so as soon as camera detects intruder, their photo is immediately taken and the action is videotaped for a few seconds.

To protect privacy Somfy's motorised shutter closes automatically when user returns home and opens when user leaves. From application, the user can open and close it as they please. Easy to Install with improved Security such as Smart Activation, system helps users arm and disarm your system.

Accurate detection with no false alarms is equipped with the best possible motion detectioncapabilities. No need to worry about false alarms, branches moving against the window or pet roaming around when user is not home. Voice-controlled with a complete range of accessories. Somfy has a wide angle for increased security with 130° wide-angle lens, Zoom x8, smoke alarm detection that recognise the sound of smoke detector and get warnings directly on smartphone. Also featured is access-sharing with auto-protection.



HunchLab

By: HunchLab | www.hunchlab.com

Used by patrol officers to identify areas of high risk for proactive patrol and focus areas are designed to change each shift to reflect the changing landscape of risk. Meter out the dosage of patrol activities to help mitigate areas from being over-policed. Mission areas designed to automatically focus on the right crimes and system knows how important it is to prevent assault versus a burglary based upon the weights that are set. Settings enable the system to reflect the values of the local community and provide a way for police departments to be more transparent about how day-to-day patrols are decided.

Working with command staff, analysts can determine the efficacy of new strategies, software utilises modern statistical methods to make experimentation and evaluation simpler and faster and departments can more easily adopt evidence-based approaches to combating crime.

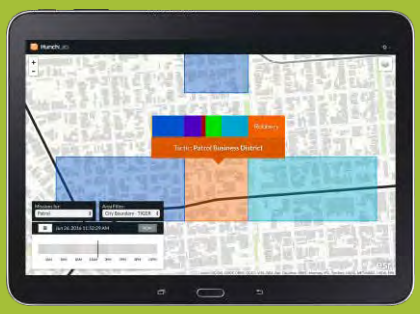
By using GPS location from MDT, smartphone or tablet, HunchLab pushes valuable contextual information to officers in field. Forecasted risk of each crime type is displayed no matter where unit is located within jurisdiction. Predictive mission areas are displayed when appropriate along with relevant tactics.

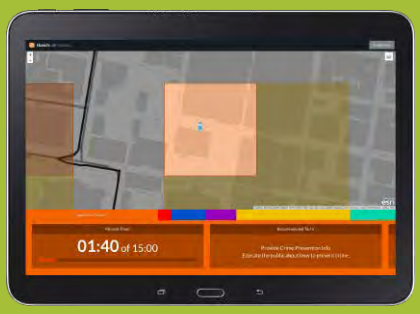
The Dashboard automatically keeps track of key performance indicators (KPIs) such as trends in event volumes and response times so that command and analysts are kept abreast of changing conditions.

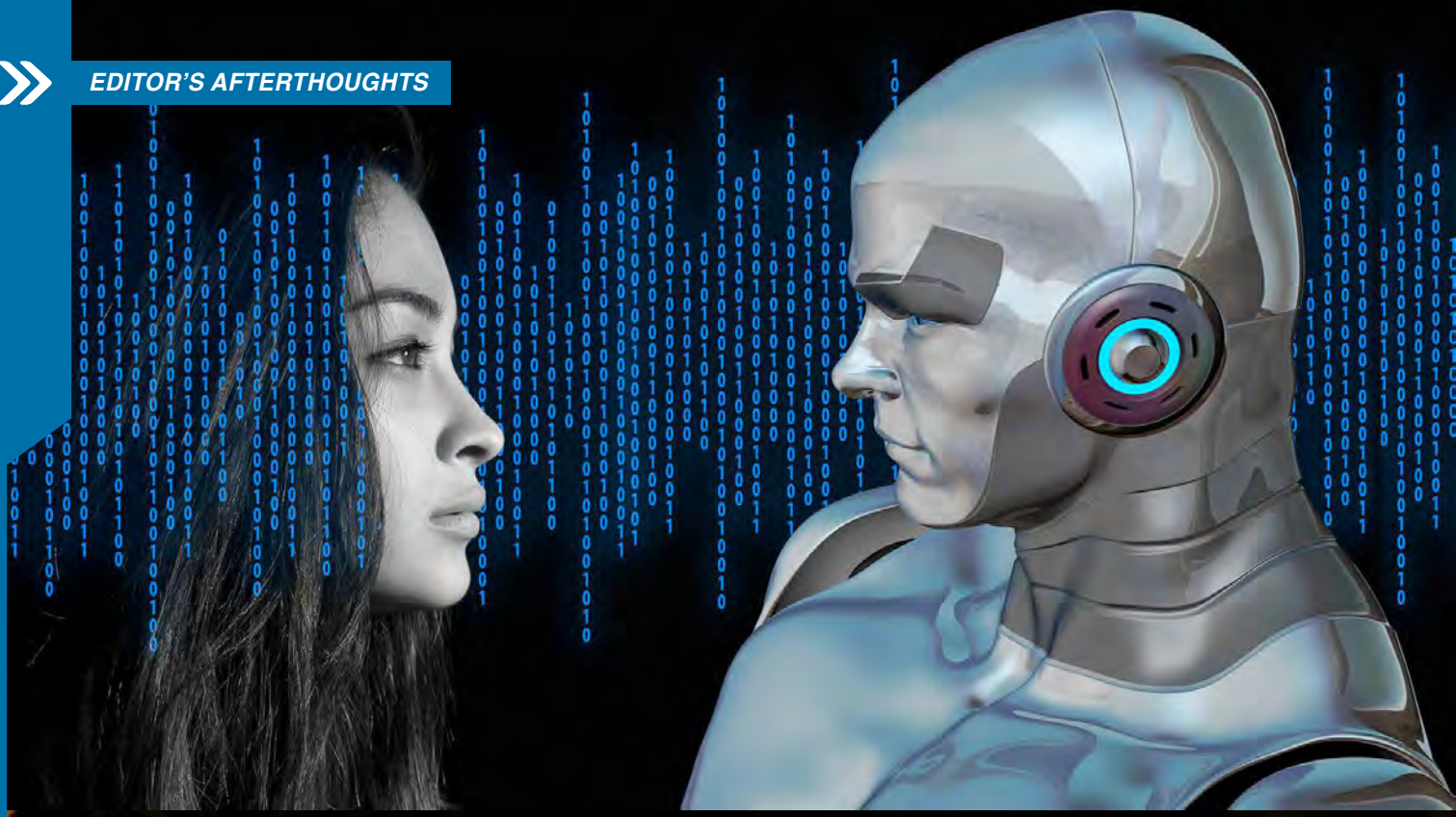
Helix3 Enterprise

By: E-Fense | www.e-fense.com

Easy to use with quick Implementation to review employee internet usage and capture screen shots and key logging. Featuring e-discovery across the entire network and sophisticated computer forensic capabilities reporting. Benefits include compliance management, cyber security,protection from employee malicious behavior, litigation support, intelligent network monitoring and is cost effective.







Fighting Crime in the SMART Nations of the Future

The Internet of Policing

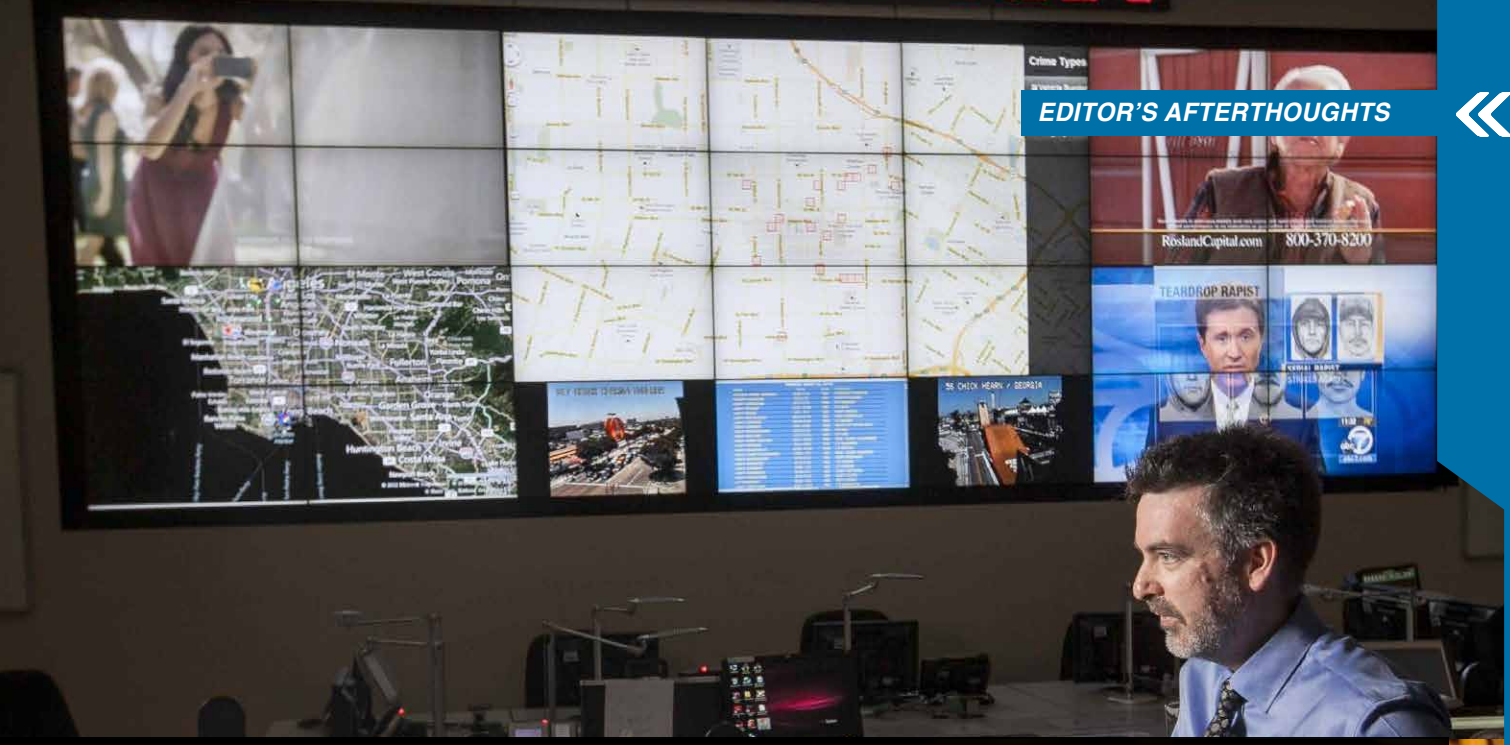
Welcome to the Internet of Everything where society is closely knit through cloud connections and the strength of social media. In an era where the world is on WIFI all day everyday, crime has evolved from the street to the information superhighway. As criminals become more and more tech savvy and digitally sophisticated, it has become an absolute necessity for law enforcement and even the military to follow suit in order to keep society safe. From predictive policing reminiscent of the dystopian film "Minority Report" to software developments and even police robots inspired by Robocop, crime fighting is evolving to meet the demands that come with securing SMART nations of the future.

Policing through Predictions

The only constant in today's society other than change is criminal activity. In order to keep up with influx of crime and the sophisticated nature of criminal activity today, it is of the utmost importance that law enforcement stay one step ahead of the perpetrators of crimes. This is where predictive policing comes into the picture via PredPol. Much like the movie Minority Report, this game-changing new technology allows police officers to be privy to crimes before they are actually committed thanks to the science of data analytics.

PredPol grew out of a research project between the Los Angeles Police Department and UCLA as a result of the need to find a way to use CompStat data for more than just historical purposes. The objective was to understand if data could provide any future recommendations as to where and when additional crimes could occur. Being able to anticipate these crime locations and times allow officers to pre-emptively deploy and help prevent these crimes. With the help of mathematicians and behavioral scientists from UCLA and Santa Clara University, the team evaluated a wide variety of data types and behavioral and forecasting models. This was broken down into 3 categories – type of crime, date and time and location where the crime will occur. "The theory is that you prevent them from committing the crime to begin with as burglars and thieves work in a mathematical way, whether they know it or not," said Modesto Police Chief Galen Carroll.

Thanks to PredPol, police have been able to Predict where and when crime is most likely to occur bas well as increase law enforcement's



odds of stopping crime. In keeping in line with the IoT, the predictions can be accessed any time and any place. As with all other security tools however, PredPol has come under fire for the risk of racial profiling. However, the technology does not Predict who will commit crimes which means there will be no pre created biases. "PredPol does not replace the experience and intuition of, but is rather an invaluable added tool that allows the police force to use their patrol time more efficiently and helps stop crime before it happens," said Chief Mark Yokoyama of the LAPD.

Robo-Cop 2017

Digitisation has also resulted in the rise of Artificial Intelligence, machine learning and robotics. While some question if there will come a time when robots will conquer humans, for now the security and law enforcement industries are merely utilising them to lighten the load efficiently for often overworked personnel. In May 2017, the world's first Robocop made its debut in Dubai as an answer to a rapidly growing population versus an insufficient amount of police officers. The robot which is bilingual currently patrols malls and tourist attractions interacting with humans who utilise it to report crimes, pay fines and get information by tapping a touchscreen on its chest.

The friendly Robocop created by Pal Robotics is also capable of broadcasting what is happening right away to the police command and control centre when crimes occur, making it easier for human policemen to be deployed to the scene of the crime.

The government in Dubai is aiming for 25% of the force to be robotic by 2030 but expressed clearly that humans would not be replaced. Like Dubai's automated police officer, there are currently a myriad of security robots on the market who perform various functions such as surveillance, facial recognition and even weapon detection as seen in Knightscope's K- series robots.

Cyber Crime Combat

From the physical realms to the cyber scape, criminals are now utilising the internet more than ever to cause havoc in the real world. One such issue is the distribution of child exploitation and abuse imagery online reflecting ongoing abuse offline. For years, law enforcement have experienced difficulties in tracking the perpetrators of these heinous crimes due to their level of technical sophistication such as encryption and private servers hidden within websites located on the dark web.

Enter Microsoft's PhotoDNA, a free service that helps identify and remove images of child exploitation online. Flipboard is one such company that utilises this technology and was quoted as saying that it is a powerful way to help protect users and young victims while helping make the Internet safer for everyone. PhotoDNA has already helped detect millions of illegal photos on the Internet with companies such as Facebook and Twitter utilising it.

Microsoft PhotoDNA has also partnered with NetClean to make Microsoft PhotoDNA image matching technology available to law enforcement at no cost to help enhance their child sex abuse investigations, empowering them to more efficiently identify and rescue victims and bring abusers to justice.

The Future

From SMART technology to state of the art surveillance cameras equipped with facial and even emotion recognition to robotics and software, fighting crime has become digitised on a whole other level. As criminals become more adept to technological advances, so will law enforcement. In the age of IoT, the battle between the heroes and villains takes place in the cloud with consequences on the ground. Welcome to the future! SST

Singapore International Cyber Week 2017 / Govware 2017
Suntec City Convention Centre, Singapore
18-21 September 2017

SINGAPORE INTERNATIONAL CYBER WEEK 2017 / GOVWARE 2017

The Singapore International Cyber Week 2017 (SICW 2017) was held at Suntec City this year as part of the local government's efforts to launch the city-state as a SMART nation. The theme for SICW 2017 was "Building A Secure and Resilient Digital Future Through Partnership" emphasising Singapore's focus on strengthening the nation's digital future through building robust local and international partnerships.

Launched by Guest-of-Honour, Deputy Prime Minister of Singapore and Co-ordinating Minister for National Security Mr Teo Chee Hean, the event hosted discussions to enhance cybersecurity cooperation and strengthen regional cybersecurity capacity building efforts. Also present at the event was Dr Yaacob Ibrahim the Minister for Communications and Information and Minister-in-Charge of Cyber Security.

SICW 2017 also showcased the 26th edition of GovernmentWare (GovWare 2017), the region's leading conference and exhibition on cybersecurity. This year, over 250 participating companies and sponsors including Palo Alto Networks, Carbon Black Inc, Imperva Inc, NEC and BAE Systems showcased their latest innovative solutions at the exhibition segment of the event. Also featured were

TRADE CONNECTION

COSELEC
A deister electronic GmbH Company

- RFID Electronic Key Management System
- Guard Tour System
- Vehicle Access Control System
- Contactless Smartcard System
- Biometrics Verification System
- Multi - Technology Card Reader

deister electronic
The RFID Company

WE THINK SECURITY
Blk 28 Kallang Place #06-12/14
Singapore 339158
Tel: (65) 6741 5200
Fax: (65) 6741 6200
RCB No: 19880111W
Email: info@coselec.com.sg
www.coselec.com.sg

This space could be yours for

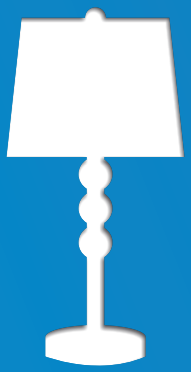
US$				Color
1x	3x	6x	9x	12x
500	440	380	320	260

S$				Color
1x	3x	6x	9x	12x
775	682	589	496	403

Scan to visit our website

We reach out to various segments of the professional readers within the building, construction, security and audio-visual industries across Asia-Pacific region with our specialised publications in print and digital formats as well as on social media platforms.

Visit our website
www.tradelinkmedia.biz
for more information.



lighting today

bathroom + kitchen today

Security Solutions Today

LAVA Lighting Audio Visual Asia

Southeast Asia building

• SOUTHEAST • ASIA •
CONSTRUCTION

TRADE LINK MEDIA PTE LTD

101 Lorong 23 Geylang #06-04 Prosper House Singapore 388399 Tel: (65) 6842 2580 Fax: (65) 6745 9517
info@tradelinkmedia.com.sg | www.tradelinkmedia.biz

country pavilions such as France, Holland, Malaysia and United Kingdom pavilions along with the Singapore Pavilion featuring Small-Medium Enterprises such as Data Terminator Pte Ltd, Netrust Pte Ltd, SecureAge Technology Pte Ltd, SuperInternet (S) Pte Ltd amongst others.

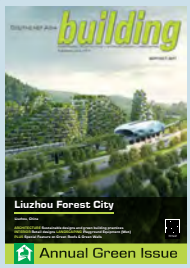
One highlight of the event was the Memorandum Of Cooperation On Cybersecurity With Japan during which Singapore and Japan signed a Memorandum of Cooperation (MOC) to strengthen cybersecurity cooperation between the two countries. Mr David Koh, Chief Executive, of the Cyber Security Agency of Singapore (CSA) and Dr Ikuo Misumi the Deputy Director-General of the National Center

Subscription Form

Fax your order today
+65 6842 2581

(Please tick in the boxes)

Southeast Asia Building



SINCE 1974

☐ 1 year (6 issues)

Singapore	S$45.00
Malaysia / Brunei	S$90.00
Asia	S$140.00
America, Europe	S$170.00
Japan, Australia, New Zealand	S$170.00
Middle East	S$170.00

Bathroom + Kitchen Today

SINCE 2001

☐ 1 year (4 issues)

Singapore	S$32.00
Malaysia / Brunei	S$65.00
Asia	S$80.00
America, Europe	S$130.00
Japan, Australia, New Zealand	S$130.00
Middle East	S$130.00

Southeast Asia Construction

SINCE 1994

☐ 1 year (6 issues)

Singapore	S$45.00
Malaysia / Brunei	S$90.00
Asia	S$140.00
America, Europe	S$170.00
Japan, Australia, New Zealand	S$170.00
Middle East	S$170.00

Lighting Today

SINCE 2002

☐ 1 year (4 issues)

Singapore	S$32.00
Malaysia / Brunei	S$65.00
Asia	S$80.00
America, Europe	S$130.00
Japan, Australia, New Zealand	S$130.00
Middle East	S$130.00

Security Solutions Today

SINCE 1992

☐ 1 year (6 issues)

Singapore	S$45.00
Malaysia / Brunei	S$90.00
Asia	S$140.00
America, Europe	S$170.00
Japan, Australia, New Zealand	S$170.00
Middle East	S$170.00

Lighting Audio Visual Asia

SINCE 2013

☐ 1 year (4 issues)

Singapore	S$32.00
Malaysia / Brunei	S$65.00
Asia	S$80.00
America, Europe	S$130.00
Japan, Australia, New Zealand	S$130.00
Middle East	S$130.00

IMPORTANT Please commence my subscription in _____ (month/year)

Personal Particulars

NAME: _____

POSITION: _____

COMPANY: _____

ADDRESS: _____

_____

TEL: _____ FAX: _____

E-MAIL: _____

Professionals (choose one):

☐ Architect ☐ Landscape Architect ☐ Interior Designer ☐ Developer/Owner

☐ Property Manager ☐ Manufacturer/Supplier ☐ Engineer ☐ Others

☐ I am sending a cheque/bank draft payable to:

Trade Link Media Pte Ltd, 101 Lorong 23, Geylang, #06-04, Prosper House, Singapore 388399

RCB Registration no: 199204277K * GST inclusive (GST Reg. No: M2-0108708-2)

☐ Please charge my credit card (circle one): Amex / Diner's Club

Card Number: _____ Expiry Date: _____

Name of Card Holder: _____ Signature: _____

of Incident Readiness and Strategy for Cybersecurity (NISC), Japan shook hands at the signing ceremony that took place at St Regis Singapore. The MOC covers cybersecurity cooperation in key areas including regular policy dialogues, information exchanges, collaborations to enhance cybersecurity awareness, joint regional capacity building efforts and in short, sharing of best practices between both countries. Mr. Koh expressed that Singapore and Japan have been working closely together on various cybersecurity initiatives at both the bilateral and multilateral levels and the MOC will serve to bring the cooperation and relations between both countries, a step further.

Mr David Koh, the Chief Executive of CSA was quoted as saying, "For governments and organisations to be able to take full advantage of the opportunities of the digital economy, cybersecurity is an essential ingredient. We hope that SICW will serve as a valuable platform for the best cyber minds - internationally and regionally - to meet, build strong networks and friendships, engage in critical discourse and access leading-edge technologies, with the aim of building a secure cyberspace for all.

All in all, SICW 2017 proved to be the quintessential event for cyber security professionals as well as security experts looking to learn about the new digitalised era of security. With the rise of ransomware, malware and other cyber attacks, both the public and private sectors have been forced to confront the issue of cyber security and this means staying ahead of the mischief makers at all times. The solutions exhibited in this show along with ever evolving technological developments provide businesses and government bodies with the tools they need to safeguard their interests. SST

ADVERTISERS' INDEX

ANTAIRA TECHNOLOGIES	19	ISC EAST 2017	OBC
CHECKPOINT SYSTEMS	5	MICROENGINE TECHNOLOGY	7
CPSE 2017	11	ROBERT BOSCH	3
DELTA SCIENTIFIC	1	SAFETY & SECURITY ASIA 2017	IBC
GENETEC	9	SECURITY CHINA 2018	15
GIGA-TMS	17	SECUTECH 2018	13
IFSEC INTERNATIONAL 2018	21	ZHEJIANG DAHUA	IFC

SAFETY & SECURITY ASIA 2017 SINGAPORE

THE 16TH INTERNATIONAL SAFETY & SECURITY TECHNOLOGY & EQUIPMENT EXHIBITION

in conjunction with

Security Industry Conference 2017

www.sic.sg

4 - 6 OCTOBER 2017
HALLS B & C
MARINA BAY SANDS SINGAPORE

Enhance your productivity through smart security solutions!

Safety & Security Asia 2017 is the quality sourcing platform for excellent commercial security solutions through an extensive array of technologies, innovations and related services in the safety and security arena. It is the most established event in the ASEAN region, as well as the longest running trade show which places focus on providing informative and strategic processes and issues related to the safety and security market of Southeast Asia.

Don't miss out on this opportunity to connect with key members of the industry through this exciting exhibition held in conjunction with the Security Industry Conference 2017!

For the latest updates, visit www.safetysecurityasia.com.sg

Book your premium location today!
ssa@cems.com.sg • (65) 6278 8666

Event Projections*

- **10,000sqm** gross exhibition area
- **250 exhibitors** from 20 countries
- **9,000 trade professionals** from 50 countries

*Combined statistics from Architecture & Building Services 2017

Organised By
Conference & Exhibition Management Services Pte Ltd

Host
Security Systems Association of Singapore

Supporting Organisations
ASIS International Singapore Chapter
Singapore Green Building Council

SIC 2017 Organiser
Security Industry Institute

Event Highlight
Merlion Awards 2017

Concurrent Events

ArchXpo 2017 The 4TH International Exhibition of Architecture & The Built Environment

iFME International Facility Management Expo 2017

LED+LIGHT ASIA 2017

Fire & Disaster Asia 2017 Singapore
The 16th International Disaster, Emergency Management & Fire Prevention Technology & Equipment Exhibition

Work Safe Asia 2017 Singapore
The 4th International Workplace Safety Technology & Equipment Exhibition

ISC EAST

SAVE THE DATE FOR
ISC EAST 2017

- 225+ Brands
- FREE SIA Education@ISC
- Crack the Tap Reception

...And more

NOVEMBER 15 - 16, 2017
JAVITS CENTER, NYC

INDUSTRY SPONSOR:

SIA SECURITY INDUSTRY ASSOCIATION

ENDORSED BY:

CASIA Connecticut Alarm & Systems Integrators Association

PBFAA

NJESA

NYSESA

security specifiers

CORPORATE SPONSORS:

AXIS COMMUNICATIONS

StarLink Fire