Security Solutions Today

May / June 2018

SURVEILLANCE GETS SMART

FROM ANALOGUE TO IP & BEYOND

Cover Focus
The Modern & Intelligent CCTV

Inside Look
The Future of Surveillance

Show Preview
Innovative Security Tech at Securitex 2018

Download our new Tradecards Global App on iOS and Android to read the latest issue!

- Temperature & Humidity Camera: Video with real-time environmental info overlay enhances monitoring efficiency.
- Gateway Camera: Connects wireless alarm devices and transmits alarm signal through coaxial cable to the XVR.
- MotionEye Camera: Motion detection & embedded PIR combine with up to 4MP video for visual alarm verification.
- HDCVI-IoT Recorder: Provides centralized IoT management with friendly UI and data reports.
- Easy HDCVI system deployment without extra wiring – saving equipment and labor costs.

Recommended Models

DH-HAC-LC1220T-TH
2MP HDCVI Temperature and Humidity Camera

DH-HAC-LC1200SL-W
2MP HDCVI Gateway Camera

DH-HAC-ME1400B/ME1200B
4MP/2MP HDCVI MotionEye Camera

DHI-XVR7000-4KL
HDCVI IoT Recorder

DH-PFM871A-N1
HDCVI IoT USB Dongle

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

May / June 2018

IN THIS ISSUE

6 **CALENDAR OF EVENTS**

8 **EDITOR'S NOTE**

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

23 **SMART TECH SECURITY RESEARCH & NEWS**
Security breaches in SMART devices and the state of cyber readiness in Singapore

39 **CASE STUDIES**
Integrated security solutions for zoos, public transport and more

40 **FUN FACTS**
Surveillance the China Way

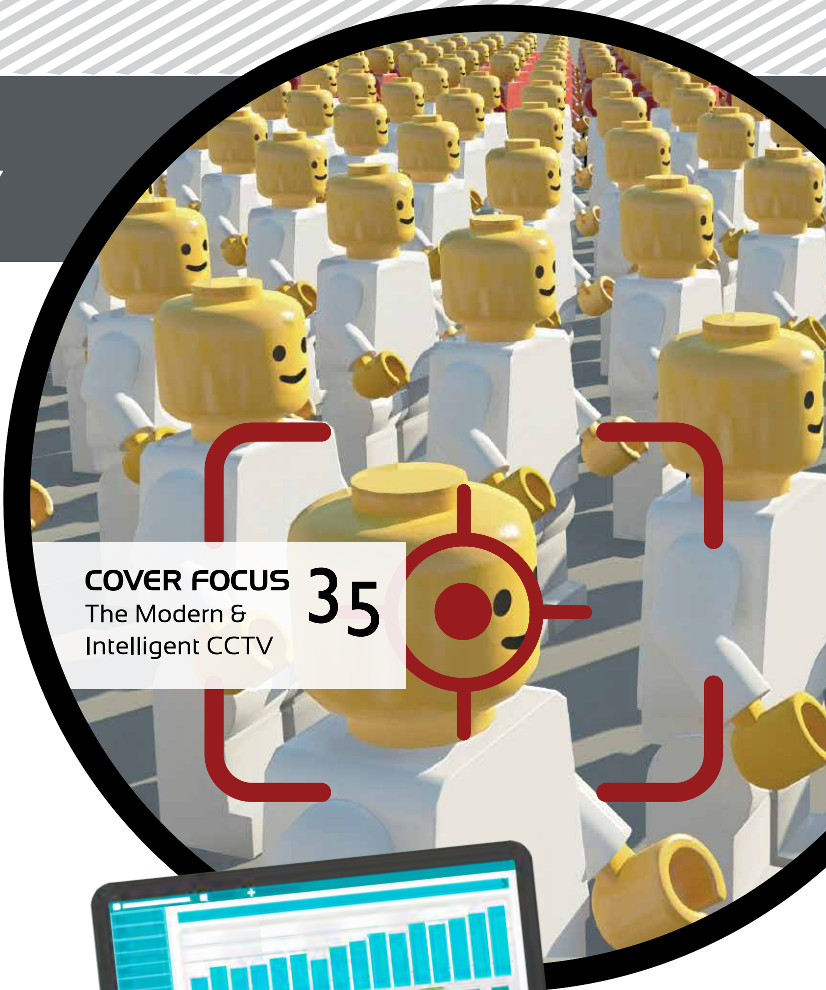
49 **INSIDE LOOK**
The future of surveillance and tech trends for the security industry in 2018

58 **IN FOCUS**
Discussing CCTV's evolution and future foresight with Soverus

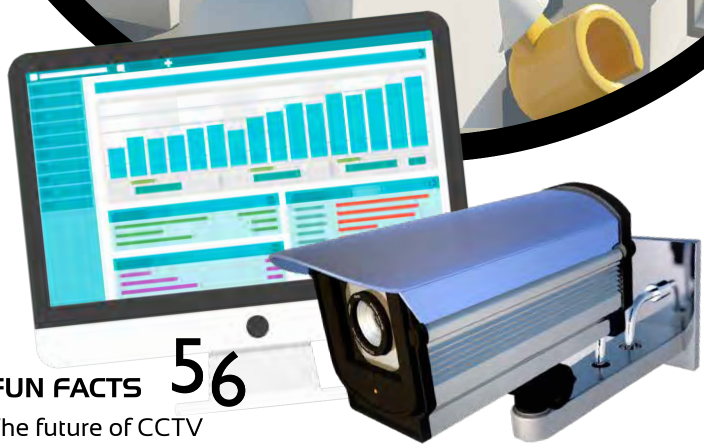
60 **FUN FACTS**
SMART CCTV, Intelligent Surveillance

62 **SECURITY FEATURES**
SMART city security, Fintec, E-commerce security and more

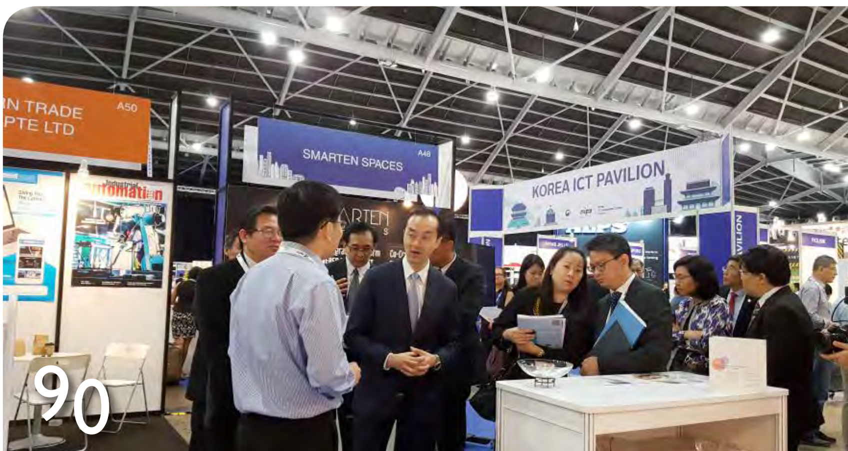
83 **SHOW PREVIEW**
A Sneak Peak into Securitex 2018 and ConnecTech 2018



COVER FOCUS 35
The Modern & Intelligent CCTV



FUN FACTS 56
The future of CCTV



90
POST SHOW REPORT
The highlights of IoTAsia 2018

CONTACT

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

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

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

MARKETING MANAGER
Felix Ooi (felix.ooi@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)

Photos/Vectors Credit: Pixabay.com / 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

COMING SOON...

MAY - JUNE

IFSEC Philippines 2018
Date: 30 May - 1 Jun 2018
Venue: SMX Convention Centre, Pasay City, Metro Manila, Philippines
Organiser: UBM
Website: www.ifsec.events/philippines

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

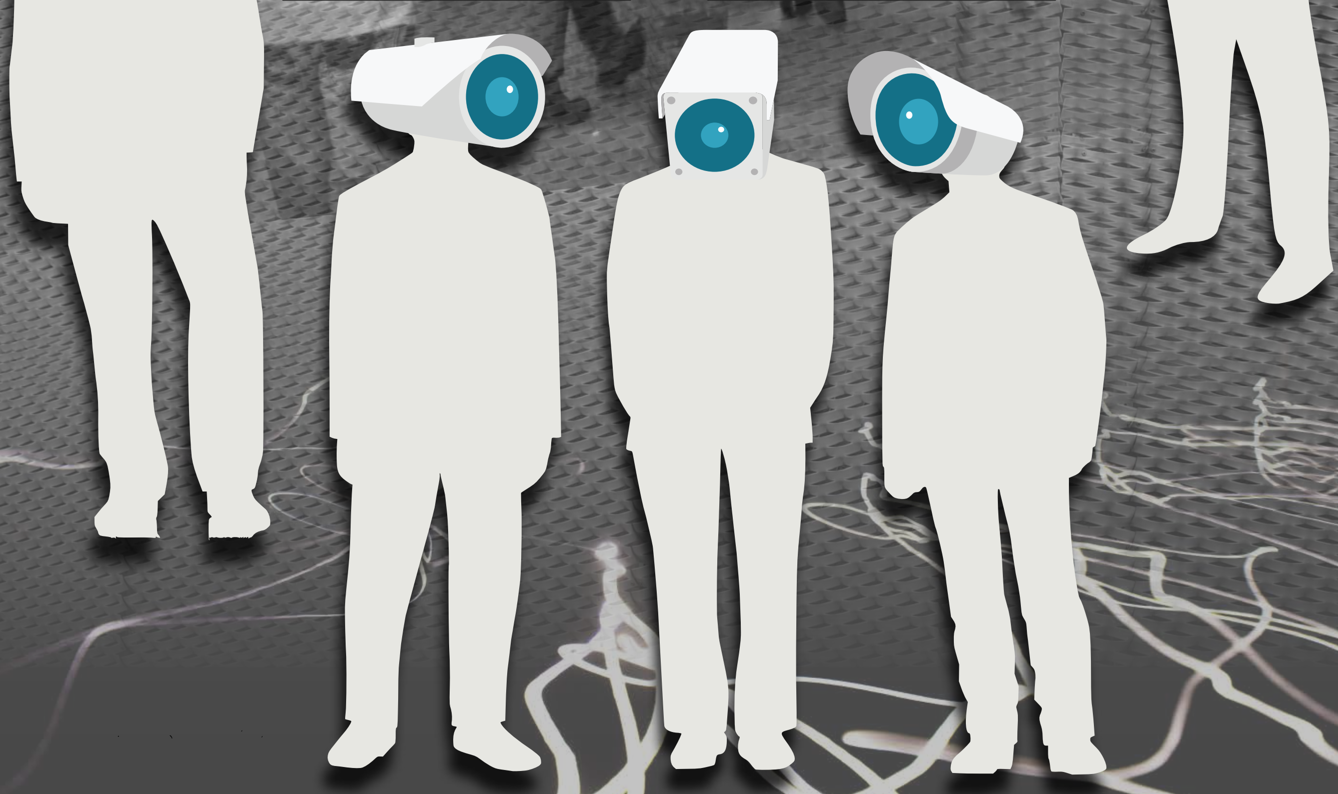
OCTOBER

Security China 2018
Date: 23 - 26 Oct 2018
Venue: China International Exhibition Centre (New Centre), Beijing, China
Organiser: China Security and Protection Industry Association (CSPIA)
Telephone: +86-10-68731701
Website: www.securitychina.com.cn
Email: International@bizcspia.com

IFSEC Southeast Asia 2018
Date: 25 - 27 Oct 2018
Venue: Impact Conventional Centre, Bangkok, Thailand
Organiser: UBM
Website: www.ifsecsea.com

DECEMBER

Counter Terror Asia 2018
Date: 4 - 5 Dec 2018
Venue: Marina Bay Sands, Singapore
Organiser: Fireworks Trade Media Pte Ltd
Telephone: (+65) 6100 9101
Website: www.counterterrorasia.com
Email: sg@asiafireworks.com



MicroEngine®

Integrated Security Systems

The Trusted Brand in Security Solutions

xPortalNet HS

High Security System Software

- 20 Digits (Full DesFire 64-bit CSN and Card ID)
- DesFire Security Profile Configuration
- Alarm Monitoring & Lift Controller
- CCTV Integration
- Visitor Management System (VMS)
- Dynamic Floor Plan for Real-Time Monitoring
- Web Server Support

Projects

Commercial / Complex

Factory

Condominium

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

Plato DesFire Reader

1300-88-3925 or enquiry@microengine.net

www.microengine.net

Our Office

Service Centre

REG No. 749921389

EDITOR'S NOTE

Dear esteemed readers,

Welcome to our May-June issue of this extremely exciting year for security technology. We are only in the middle of 2018 and already technological developments on the security front are developing rapidly specifically in the field of Artificial Intelligence, machine learning and robotics. All these advancements are slowly but surely being applied to CCTV cameras, surveillance software, access control devices and the like. On this note, we would like to welcome you to the era of SMART surveillance. The digitalisation brought about by the Internet of Things has touched every aspect of our daily lives and security is no exception in this. The fact that criminals are becoming more tech-sophisticated demands that the security industry evolves accordingly to safeguard property, facilities and people. The issue of cyber security has gone from the IT desk to the world at large because we are no longer are dealing with viruses that can crash a computer or two but full scale security breaches that can bring down an entire facility. This is where video analytics, biometric software such as facial recognition and even license plate identification software come into play.

In this issue, you will be exposed to the SMART revolution of security cameras in a sense that CCTV surveillance is no longer utilised simply to monitor and provide evidence of a possible breach after or during the event but utilised intelligently or in a SMART manner to predict and therefore prevent the crime or breach before it even happens. This is done via surveillance software equipped with facial recognition, voice recognition and even sets of complex algorithyms that detect patterns in behaviour and other data from video surveillance footage in order to prevent security breaches effectively.

The current trending topic in the world of CCTV and video surveillance in general is the usage of SMART surveillance in public safety. Every day we read about the creative and incredibly innovative ways in which countries like China and the United states are utilising surveillance cameras to safeguard the public as well as secure private facilities. This is seen in the emergence of autonomous security robots, drones and of course video analytics. Technology is indeed taking security to places that human beings are unable to physically traverse.

Thanks to this SMART software, video analytics has created the opportunity for CCTV to be utilised not merely for security but for other purposes as well such as marketing and retail analytics due to its ability to track how many people enter a building or area, how long people stay in certain areas. Apart from predictive policing and the like, cameras are now equipped with software that goes beyond monitoring and enters the realm of facial and emotion analysis. Other than humans, vehicles are also under the ever-scrutinising eye of the camera. The magic is in the patterns and this means more efficient protection.

In our Case Studies section, we will look at how security integrators such as Northrop Grumman and Tyco are providing solutions provide multiple levels of security both digital and physical to meet the needs of a diverse range of clients such as zoos, public transportation and even a veteran's medical facility.

Our Inside Look section this issue focuses on the upcoming surveillance trends of 2018 such as biometric applications, cord-free utilities and of course cyber security proofing features which have become incredibly important in this era of the Internet of Things. We will also be exploring the tech trends in general for the Security Industry as a whole, specifically Artificial Intelligence, Machine Learning and more. These technologies have revolutionised how security is safeguarded and secured and will continue to do so in 2018 and beyond.

In this issue's edition of In Focus, we converse with a representative from security solutions provider Soverus. Equipped with years of experience in the industry working with various sectors such as homeland security and the police, Miss Tan Khai Hua the Head of Marketing and Communications shares with us her opinions on a myriad of topics concerning CCTV cameras such as the switch from analogue to IP, the usage of video analytics in crime prevention and of course the current craze of robotics and drones which are said to be possible replacements for human security guards in current times as well as the near future.

Also included in this issue are our informative spreads chock full of fun facts on the present state of the security industry. From China's innovative usage of CCTV cameras in everything from fast food outlets to traffic violations, future tech of CCTV and all about analytics. We are confident that you will enjoy these tidbits of information that we have assembled.

I certainly hope that you will enjoy this informative issue as much as I have enjoyed curating the current trends and future predictions for your reading pleasure. We look forward to bringing you even more industry developments in the years ahead and thank you for your continued support. 2018 will most definitely be a revolutionary year for security and we will most definitely be bringing you all the highlights, every step of the way.

Melissa T
Editor

Delta's New **TB100** Crash-Certified Portable Bollard Systems Help Stop Vehicle Massacres

Now, Delta's new patent pending TB100 moveable bollards will help you stop terrorists and errant drivers from causing mayhem on roadways as narrow as bike paths or as wide as airport runways. Tote them into place onto any stable surface such as concrete, asphalt, compacted soil or vegetation and installation is done. No excavations or sub-surface preparations are required. Link together five TB100 portable bollards with a cable system or use individually.

Keep your people safe. A TB100 portable bollard system will stop and disable a 15,000 pound (6,804 kg) vehicle traveling at 30 mph (48.3 kph), resulting in an ASTM M30, P3 rating. A single TB100 bollard absorbs 400,000 foot pounds of kinetic energy with a hit coming from any direction. Portable bollards can be used in conjunction with Delta's popular MP5000 portable barricade to fill gaps in the roadblock.

Don't gamble with your people's welfare. Bet their lives on Delta.

DELTA

Visit **www.deltascientific.com** for full details and specifications. ▲ **1-661-575-1100** ▲ **info@deltascientific.com**

New Technology for Smart Cameras Delivers Improved Object Recognition in Sub-optimal Lighting Conditions Developed in Ben-Gurion University

The novel software app can be added to any smart camera and used for various applications, including face recognition for security and augmented reality

Beer-Sheva, Israel - BGN Technologies, the technology transfer company of Ben-Gurion University, announced today that researchers at Ben-Gurion University of the Negev (BGU) have developed a new Light Invariant Video Imaging (LIVI) software technology that can significantly improve picture clarity of cameras in sub-optimal lighting, thus enhancing object recognition. The new software app can be added to any existing smart camera system for various applications, including facial recognition for security use, as well as augmented reality.

LIVI increases the functionality of cameras by eliminating the effects of background or dynamic lighting conditions, thereby delivering shadow-free images with constant color output and improved contrast. The software relies on amplitude-modulated (AM) light separation, similar, in principle, to AM radio communication. This enables cameras to separate the influence of a modulated light from unwanted light sources in the scene, causing the AM video camera frame to appear the same, independent of the light conditions in which it was taken.

"Strong background light creates shadows, for example when people walk into buildings, interfering with the ability of our eyes and cameras to recognize faces," said Prof. Hugo Guterman, from the Department of Electrical and Computer Engineering, and head of the BGU Laboratory of Autonomous Robotics. "Our invention produces a 'flash' effect that clears the backlight, removes shadows and improves contrast, making all captured frames much clearer," says Prof. Guterman. "This can have numerous applications, from smart security cameras through cell phone or computer face recognition apps, augmented reality and video game applications and military use."

Amir Kolaman, a Ph.D. student at the Department of Electrical and Computer Engineering, was working on his thesis on underwater photography when the issue of backlight arose. Together with Prof. Guterman, they developed the system that filters out the backlight for each pixel in the image, much the same way that a radio receiver filters one station from another. "Light intensity can be modulated at different frequencies just like in radio waves," says Kolaman. "We turn each camera pixel into an AM receiver that tunes to the flash light and filters out the background lights from the output frames."

According to Netta Cohen, CEO of BGN Technologies, "This is a perfect example of a technology developed at BGU labs that addresses real market needs. This new technology is inexpensive to produce and can be easily incorporated into various devices." BGN Technologies is now seeking a partner for the further development and commercialization of this breakthrough technology.

The video analytics market is most likely the first market in which the technology will be integrated, since robust camera frames improve performance of facial recognition and identification. The global video analytics market is projected to reach $11.17 billion by 2022 according to a Markets and Markets report published in April 2017.

The recreational smartphone market represents another major opportunity, as more smartphones come equipped with facial recognition security. The worldwide smartphone market reached approximately 1.53 billion units in 2017, according to an IDC report published in March 2017. SST

Entrust Datacard Earns Blue Shield Technology Innovation Award from the China International Association for Promotion of Science and Technology

Receiving China's top security award cements Entrust Datacard as a leading security provider in the market

Minneapolis, USA -Entrust Datacard, a leading provider of trusted identity and secure transaction technology solutions, announces that the company has received the Blue Shield Technology Innovation Award for Security and Anti-Counterfeiting Technology for the Entrust Datacard™ Retransfer Card Printer series from the China International Association for Promotion of Science and Technology (CIAPST).

Established in 2010, the Blue Shield Technology Innovation Award for Security and Anti-Counterfeiting Technology was created to promote the innovation and application of security and anti-counterfeiting technology by companies around the world that conduct business in China, and is now viewed as the top award in the Chinese security industry.

Entrust Datacard received the Blue Shield Award for its Retransfer Card Printer series at the 12th Security Document Summit in Beijing, China. This on demand solution gives financial institutions, enterprises, universities and government programs the flexibility and features they need to issue identity, access and payment cards – right from their desktop. The printer provides long-lasting, high-definition images, while ensuring a deep level of security, durability and reliability.

"It's an honor to be recognised as a leading security solution provider in the Chinese security industry and to have the Retransfer Printer series recognised as a top product in the market," said Angus McDougall, regional vice president – APAC for Entrust Datacard. "We're pleased to see that the Retransfer Printer series have not only provided a flexible and reliable identity platform, but has also redefined printing expectations for both our customers and the industry as a whole."

This recognition is the result of Entrust Datacard's 48 years of security expertise and over 20 years of providing trusted identity and transactions in China. In 2017, for example, Entrust Datacard reduced turnaround time from 30-45 days to the same day for a social security card issuance program across various provinces in China. This was achieved through an in region partner that implemented retransfer printers in a variety of provincial issuing locations.

"Entrust Datacard is dedicated to providing the most innovative printing solutions to our customers in China," said Angus McDougall, regional vice president – APAC for Entrust Datacard. "This effort will continue as we enhance the capabilities of our retransfer printers and overall printing portfolio."

Entrust Datacard offers a suite of desktop printers designed to provide card issuers with a unified solution for issuing identity credentials. These printers include the Entrust Datacard™ CR805™, CR825™ and CE875™ Instant Issuance Systems which makes up the Entrust Datacard ultimate identity platform. SST

Entrance Security Swings into Action with Boon Edam's Ultra-Slim Speedlane Swing

Boon Edam's Speedlane Swing is the slimmest speed stile in the range

Sydney, Australia - Entrance security has evolved in the last decade to a point where functionality alone is no longer enough. Architects, engineers, facility managers, security consultants and other specifiers are seeking elegant and refined solutions to manage the follow of people into, out of, and around buildings and facilities.

Boon Edam's Speedlane Swing, part of its Lifeline series of speed stiles, has been designed to perfectly blend high quality engineering, with elegance and sophistication, to provide a modern entry, suitable for high rise buildings, corporate HQs, broadcasters, treasuries, diplomacies, embassies, legislature, parliaments and other government buildings.

The Speedlane Swing, which will be on display at the 2018 Security Expo in Melbourne (Stand G2) this July, is the slimmest in the Lifeline Series – which also includes Open and Slide models – with the cabinet housing measuring as little as 106mm. The slim nature of the speed stile makes it ideal for narrow entrances, where multiple lanes can still be installed to guide visitors smoothly through the space.

"The small cabinet housing is a major advantage of the Speedlane Swing model. We've worked on a number of projects where an additional lane can fit using a Swing model, that would not have been possible with larger units," says Mr Alastair Russell, National Sales Manager, Boon Edam Australia, who has over 30 years of experience in entrance security, both in Australia and the UK.

Energy-efficiency is built into the Speedlane Swing, which has sensors to determine if anyone is within range. If enough time has elapsed with no activity, the unit goes into a 'sleep' mode where lights are turned off to save power. As soon as someone walks within the sensors range, intuitive lighting switches on and guides the user effortlessly through the gate.

"The Speedlane Swing has been designed to be as user-friendly as possible. Modern arrow symbols guide users simply and effectively into the correct lane and prevent any confusion," says Mr Russell.

"The Speedlane Swing can also be used as a second-tier security system, in multi-layered security buildings, where primary barriers are set up further inside the facility," he said.

BoonTouch

A universal 'BoonTouch' control is available for applications where the Speedlane is used in conjunction with a manned security operation. The security team member is able to control any combination of up to six security access solutions. With a user-friendly interface, BoonTouch allows for the control of individual lanes, multiple lanes and to control an alarm situation.

"The BoonTouch feature is ideally suited to the front entrance of a building where the majority of visitors will have passes to swipe on the Speedlane, but there will be occasional visitors who will need temporary passes or assisted access," says Mr Russell.

"BoonTouch allows for all units to be held open for open days, or locked down in the event of an emergency, giving greater control to the security team," he said.

Speedlane Features

The Speedlane Swing has been designed to the highest standards and incorporates a range of modern features, including using unique sensors, which detect visitors approaching. sleep function to save energy, pulsing light strips to guide the user, intuitive and proven symbols to make it user friendly, ergonomic design for customer comfort, customisation possibilities in fitting with interior design and premium quality materials. SST

The international exhibition & conference on building maintenance and facilities management

BMAM EXPO ASIA 2018

12-14 SEPTEMBER 2018

HALL 5-6, IMPACT, BANGKOK, THAILAND

INTEGRATED FM OF THE FUTURE

BMAM Expo Asia 2018 offers exciting possibilities for businesses keen to be at the forefront of innovation and technology in facilities management.

EXHIBIT NOW!

FM Products & Services I Plant Maintenance I Facilities Management Software
Workspace Management I Smart Building Solutions I Cleaning Products & Services
Security I Interior & Landscape Design I Green Building Technologies I Health & Safety

Scan to book your booth

Organized by IMPACT MUANG THONG THANI

www.bmamexpoasia.com

BMAM Expo Asia

+66 (0) 2833 5208

Agilent Wins Security Innovation Award

ADS Group Recognises Unique Handheld Raman System

Santa Clara, California, USA - Agilent Technologies Inc. today announced that it has received the ADS Security Innovation Award for the company's Resolve handheld Raman system. The Resolve system rapidly detects explosives, narcotics, and other hazardous materials through unopened, opaque containers.

The ADS Group represents companies in the aerospace, defense, and security sectors in the United Kingdom. The award-winning product was developed by UK-based Cobalt Light Systems, a provider of highly differentiated Raman spectroscopic instruments, which Agilent acquired last year.

"We are delighted to receive this award for security innovation," said Dr. Paul Loeffen, director of Raman spectroscopy at Agilent. "Resolve's through-barrier detection capability is a real game-changer in handheld chemical detection. Resolve systems are now deployed at ports and borders around the world for law enforcement, military, hazmat, and customs applications."

Conventional handheld systems are effective through clear plastic bags or clear glass vials. If materials are concealed behind colored or opaque barriers, it can be necessary to open the container and take a sample—exposing the operator, and possibly the public, to increased risk.

The Resolve system adds a unique capability, using spatially offset Raman spectroscopy (SORS) to identify explosives, narcotics, toxic chemicals, chemical warfare agents, and more, through colored plastic and glass, paper, fabrics, and other packaging materials.

"Resolve helps protect the people who protect us," Loeffen added.

Resolve is also aiding law enforcement and customs officers in the fight against synthetic opioids such as fentanyl. The system can detect fentanyl and its analogues through opaque packaging. SST

Mutualink to Provide Real-Time Video Enhancement Technology that "Sees through Fog, Smoke, Snow and Lowlight Conditions"

Orlando, Florida, USA -Today, Mutualink, Inc., a worldwide leading provider of secure interoperable communications solutions, announced an exclusive master licensing partnership with Orlando, Florida based ProHawk Technology Group, Inc. that will enable Mutualink to deliver new powerful real-time video enhancement technology to the US public safety and FirstNet customers. ProHawk Technology enables live streaming video obscured by environmental conditions such as fog, darkness, snow, and smoke to be enhanced and corrected to provide views of hidden or obscured objects in near real time, under 20 microseconds. The ProHawk capability will be integrated into Mutualink's interoperable communications and media sharing platform and will also be made available to Mutualink's video integration partners. The patented technology can work with any standardised video camera stream source output or remotely in the cloud.

"The ProHawk real-time video enhancement capabilities are incredibly impressive and there are many valuable applied uses for the US first responder community," said Mark Hatten, CEO of Mutualink, Inc. "The ability to see objects and persons of interest otherwise hidden from normal view due to prevailing conditions provides smart cities, public safety and emergency responders with critical information that would otherwise go undetected." Public security video cameras and other surveillance assets are outdoors, typically hanging from infrastructure or mounted on vehicles, aircraft and drones. "Every day is not a perfect viewing day and in the case of disasters there is significant likelihood of less than optimal viewing environments being present. This makes this technology especially relevant and needed," according to Hatten.

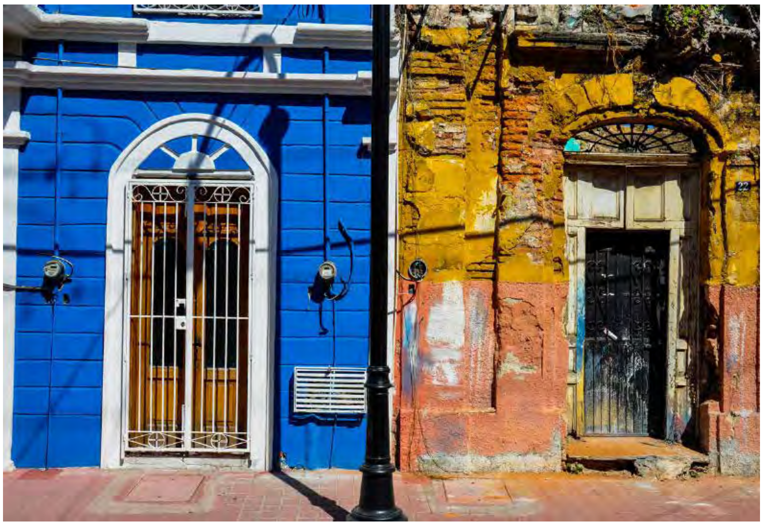
According to Joe Seebach, Chief Commercial Officer and founder of ProHawk, the video enhancement technology is unlike anything else available in the market. "Our patented technology operates on a sophisticated one-pass algorithm that enables nearly instant processing and enhancement results. The initial use case for our technology required video enhancement to be simple to use, reliable, and real-time or the consequences could be deadly in real-time security or crisis situations," said Seebach. He also pointed out that the ProHawk technology is necessary for any real-time Artificial Intelligence analytics and sensors. "ProHawk technology clarifies video in real time and then it can be passed to machine vision processing with significantly better results. We've seen this work especially well in low light license plate recognition (LPR) and facial recognition systems."

Under the Mutualink-ProHawk partnership, Mutualink will make ProHawk technology available to the US public safety community and FirstNet users on an exclusive distribution basis. ProHawk's technology has already been tested and is in use in defense applications and other environments. Parties interested in ProHawk real-time video enhancement solutions may contact ProHawk or Mutualink to inquire. SST

Vicon Delivers Statewide Surveillance Solution in Mexico

Sinaloa Government Chooses Valerus for Its Multi-City Network

Hauppauge, New York, USA - Vicon Industries, Inc., designer and manufacturer of video surveillance and access control software, hardware and components, announced today that it is working closely with the State of Sinaloa, Mexico to create a statewide surveillance network that unifies the systems of all of its metropolitan areas, including the cities of Culiacan, Mazatlan, Los Mochis and others. The new statewide initiative, built upon Valerus VMS software, will allow for greater coordination between all municipalities and their law enforcement agencies in their efforts to combat the influence of powerful drug cartels entrenched within the region. Valerus' 100% web-based and true open standards VMS software will provide the state with a more secure, responsive environment capable of providing a single-seat view of its entire security domain.



A new, state-of-the-art facility in Culiacan, the state's capital, serves as a centralised coordination hub for security and life-safety operations at the city, municipal and state levels. Expansive video walls, recording servers and monitoring stations provide operators with access to all cameras within their respective domains, with the ability to share video across departments as necessary. There are currently over 1000 Vicon security cameras in Culiacan, along with 800 special license plate reading cameras custom developed by Vicon for this project. Ultimately, there will be approximately 4800 cameras in Culiacan alone, with thousands more across the other cities.

M.C. Jose de Jesus Galvez, the state's Secretary of Innovation and close aide to the Governor, says that Vicon's Valerus is able to provide a centralised system, with localised control and operation, which is flexible enough to work with much of the equipment already in place in each city. Plus, the cost to purchase and install Valerus was less than for other video management systems, providing long-term, recurring savings that he will then be able to invest in additional equipment and system expansion over time.

Maria Bustamante-Prada, Vicon's International Sales Manager, explains, "Vicon has successfully supported the city of Culiacan's security needs for many years, and our proven commitment to customer satisfaction was an important factor in earning the confidence of the state. This is a huge investment for them, and they know that we will be there to support them at every step."

"This is a very ambitious project for us," says M.C. Galvez. "We hope to use every function of Valerus to help lower the crime rate and better protect the citizens of Sinaloa. We understand that video isn't the only way we will achieve this, but it's a very important part and can help us bring other systems together to be more effective. We're excited about the possibilities." SST

Panasonic to Launch Face Recognition Server Software Using Deep Learning Technology

The Face Recognition Server Software WV-ASF950 and the Face Registration Expansion Kit WV-ASFE951W will be launched in July outside Japan and in August 2018 in Japan

Osaka, Japan - Panasonic Corporation announced that it will release face recognition server software using deep learning technology in July 2018 outside Japan and in August 2018 in Japan.

Featuring a core engine that boasts the world's highest face recognition performance, this high-precision face recognition software can identify faces that are difficult to recognize with conventional technologies, including faces at an angle of up to 45 degrees to the left or right or 30 degrees up or down, and those partially hidden by sunglasses.

In addition, the new software features the "iA (intelligent Auto) mode" that automatically adjusts settings for the camera to shoot optimal images best suited for face recognition. When it is used with Panasonic's i-PRO EXTREME series network cameras installed with the "Best Shot License Key" that comes bundled with the software, only the "Best Shots" will be sent to the server for face recognition. The combination of Panasonic core devices and the face recognition software maximises the performance of the software's core engine to achieve high-precision recognition. The company plans to add a function to recognize partially covered faces with a surgical mask, which is difficult with conventional systems, by the end of this year.

Furthermore, using this software with cameras equipped with the iA function enables image analysis to be performed on the camera instead of the server to send only the best images to the server. This will result in reducing server and network loads, which leads to overall system cost reductions. In the case of 10 or more network cameras are connected to the system, the costs can be reduced by about 40 to 50% compared to conventional systems that do not use the Best Shot function.

Panasonic will continue to improve its security-related products and provide various solutions to meet increasingly diversifying and evolving customer needs, such as face recognition solutions for integrated management with a monitoring system. By providing these solutions, the company is aiming to become a "total integrator" capable of contributing to customers' frontline operations.

With the rapid popularization of IoT and AI, initiatives for connecting various types of information to make life more convenient are taking place in every industrial sector. A new technology called "deep learning" is being utilised in order to achieve this. Panasonic has adopted this deep learning technology in its face recognition products for the security industry. This has led to the successful development and commercialization of the face recognition technology that overcomes the difficulties of conventional technologies, such as recognising faces when they are tilted, changed by aging, or partially hidden with sunglasses.

Panasonic will offer this product as a personal recognition solution for video security in various situations, such as the monitoring of public facilities and entry management.

Facial recognition server software

Singapore's Leading Security Solutions Provider Ademco Partners IE Singapore to Make First Acquisition in Vietnam, With Aims to Increase Overseas Revenue by 50% to Drive Total Business Growth

Singapore - Ademco Security Group Pte Ltd (Ademco), one of the region's leading providers of security and business management solutions, today announced its 60% acquisition of TNT Technologies Joint Stock Company (TNT), Vietnam's market leader in high-end integrated security solutions , in partnership with International Enterprise (IE) Singapore. This marks Ademco's first Vietnam acquisition in a move to build local presence to capture Vietnam's growing needs for integrated security solutions in business operations and management. Today, overseas investments account for about half of its S$40 million annual turnover. Ademco expects to further increase its overseas revenue by 50% over the next three years to drive business growth; Vietnam will be a key contributor to this through the acquisition.

Delivering integrated innovative and comprehensive security solutions to more than 8,000 institutional, commercial and government clients across Asia for more than three decades, the entry into Vietnam is the seventh addition to Ademco's growing geographical footprint across Singapore, China, India, Indonesia, Malaysia and the Philippines. It plans to establish a regional presence in 14 markets globally by 2020.

TNT is a 12-year-old company providing high-end integrated security solutions to clients across aviation, banking, manufacturing, oil and gas, and retail. It has a respected track record, with notable projects for clients such as the Hanoi Noi Bai International Airport, Samsung Electronics Vietnam and Mektec Manufacturing Corporation2. The acquisition enables Ademco to draw the deep market knowledge and expertise of TNT, build stronger local presence and reach through its extensive MNC client base in Vietnam, as well as strengthen operational efficiencies through the sharing of best practices and technical know. TNT will also be able to further increase its local reach to the MNC client base with Ademco's added solutions.

Ademco is working closely with IE Singapore on its internationalisation strategy. The Vietnam acquisition was supported by IE Singapore, which provided in-market information on the industry landscape, and facilitated the critical pre-acquisition due diligence process. The in-market assistance helped Ademco make a better assessment on the market potential and the right timing for the acquisition.

Mr Toby Koh, Group Managing Director of the Ademco Security Group, said, "Overseas expansion has always been our catalyst for growth and we are very bullish about the opportunities that Vietnam presents. Not only is there a strong demand for integrated security management systems by large MNCs with regional operations in Asia, we also see great potential in the large local enterprises and government bodies, who are slowly beginning to recognise the advantages of unifying and enhancing their security efforts to achieve greater operational efficiencies at a lower cost."

Vietnam registered an increase in Foreign Direct Investments (FDI) of 44% over the past year, totalling over S$46.9 billion in 20173. Its large workforce, low cost structure and government support has attracted many international corporate offices, manufacturing, logistics and warehouse operations. As a result, there is a corresponding increase in demand for high-end and integrated security solutions and services.

Mr Koh added, "Key to Ademco's international success has been our engineering expertise, solutioning know-how and our ability to leverage on the trust and credibility that comes with being an established Singapore brand. This has been further enhanced through our close relationship with IE Singapore, who has not only been instrumental in providing critical pre-acquisition due diligence support in Vietnam, but also in helping us scale up our business expansion strategies in India and China through important business contacts and market intelligence."

Ms Sophia Ng, Group Director for Technology Business Group, IE Singapore, said, "Mergers and acquisitions allow Singapore companies to gain new capabilities, become more efficient through the sharing of best practices and gain strong local partners who can strengthen their overseas reach. Ademco's partnership with TNT is a good example of a strategic move to speed up the process to establish a local presence overseas to drive greater growth."

Beyond Vietnam, Ademco is partnering IE Singapore to scale up in Asia including India and China. Key to Ademco's regional growth strategy will be its ability to support and enhance the operational efficiencies of its overseas offices. This will involve further investment in the building up of the finance and manpower capabilities within its Singapore headquarters, which is supported by SPRING Singapore. Ademco is also investing to further strengthen their regional development, engineering and solutions (DES) resources. SST

Dahua Technology Releases Consumer Products Globally with the Brand Lechange

Hangzhou, China - Dahua Technology, a leading solution provider in the global video surveillance industry, releases consumer products with the brand Lechange, to serve families desiring better safety and greater convenience as well as SMB (small and median business) owners globally.

Lechange cores in technology and design. Armed with Dahua's technology in video surveillance industry, Lechange enables consumers to better enjoy technological advancements including high definition, facial recognition, voice recognition, artificial intelligence and cloud storage. With good design applied in hardware and software, Lechange assures excellent user experience during installation and daily use.

Lechange introduces altogether 7 products to the international users, including Cue/Cue 1080P Wi-Fi Cameras, Ranger/ Ranger 1080P Wi-Fi Pan & Tilt Cameras, Bullet 1080P H.265 Wi-Fi Camera, Ranger Pro G 1080P H.265 Wi-Fi Pan & Tilt Camera with Airfly and DB10 Wi-Fi Video Doorbell. The first batch of Lechange products delivers multiple functions including surveillance, remote monitoring, smart appliances and advanced analysis.

Family members, for example parents and kids, can be safeguarded by Lechange system which is easy to set up and compatible with Smart Home systems, with round-the-clock safety and more flexible access control as well as HD video surveillance for the family members. You can also interact much more and easier with them, including pets, using Lechange products.

SMB store managers can now monitor the conditions in their shops more conveniently and comprehensively. There is an additional benefit for Lechange users, as they can record the video of funny or precious moments and share them on the social network.

"We first launched the brand in 2014 in China and it quickly became a beloved home security brand highly regarded by customers," Li Jiang, product manager for Lechange, said, "and now, with experience accumulated and technologies updated, we'd love to bring our advanced and proven products and solutions to global users." With true values delivered to families and SMBs, Lechange is perfecting daily life. SST

TeleEye Launches Starlight MP2300 Series IP Cameras that Meet the Budget of Small and Medium-Sized Businesses

Hong Kong - TeleEye, the global leading supplier in video surveillance systems, is pleased to announce the introduction of the new MP2300 Series starlight network camera to their extensive camera product line. The MP2300 Series features 2MP resolution and adopts Sony starlight CMOS sensor, providing a high and reliable performance for day and night surveillance with a competitive price. The MP2300 Series family comprises of 4 camera models with different designs and features, and yet, all of the cameras integrate with TeleEye's dedicated technologies. Therefore, this series is able to cater for various security needs and surveillance applications. With a user-friendly design, the MP2300 Series is easy to be installed as well, enabling a higher flexibility during deployment.

Equipping with Sony Starlight CMOS Sensor

The MP2300 Series equips with Sony Starlight CMOS Sensor, enabling a higher sensitivity to various lighting conditions. As a result, not only can it capture quality video images during daytime, it is also capable of delivering superior performance even in extreme low light settings. The MP2300 Series is ideal for a range of indoor and outdoor applications, and meanwhile meeting the budgets of small and medium-sized businesses.

Integration with TeleEye's Advanced Technologies

The MP2300 Series integrates with TeleEye's dedicated Dynamic I-frame Technology (D.I.T) and Dynamic Resolution Technology (D.R.T) to enhance video optimization in regard to the recording time and bandwidth efficiency.

As regards TeleEye's D.I.T, this technology will intelligently do the data analysis based on the environments to adjust the frequencies of I-frames and P-frames. During the recording, this smart technology will automatically determine the frequency of I-frames according to the motion sequence of the scene. As a result, data storage can be greatly saved for a longer video recording time.

While with TeleEye's D.R.T, the resolution of the videos regardless of size will be automatically adjusted in the video management platform in accordance with the chosen number of screens. The resolution of the videos will be decreased with the increasing number of screens, thus, the video volumes can be minimized to increase bandwidth efficiency. Even with a limited bandwidth size, a smooth video stream can still be guaranteed under this intelligent technology.

Various Camera Choices for Different Security Needs

The MP2300 series have 4 camera models, respectively equipping with a 2.8mm fixed lens with IR illumination range up to 20m, and a 2.8-12mm vari-focal lens with IR illumination range up to 30m. This series is available in both dome and bullet models.

Easy Installation

The MP2300 Series adopts a user-friendly design, in which the security installers will benefit from the easy installation as the cameras can be easily mounted and adjusted on walls without opening the exteriors. The flexibility during the deployment is enhanced. SST

Abloy UK Launches Cliq Go App

Security expert Abloy UK has launched the new CLIQ® Go App, designed to allow small to medium sized organisations to remotely manage their security from wherever they are, keeping their business secure 'on the go'.

Managing a business today comes with a many security challenges, and the needs of the business may be constantly changing and evolving. For example, staff leave, new staff join, keys are lost and access rights need to be changed.

The CLIQ Go App moves security to a new dimension, enabling business owners to control security in their building and premises from their mobile device.

Features include the ability to schedule access to rooms or give contractors time-limited access. If a key is lost, access can also be revoked using the CLIQ Go App, all managed from a cloud-based system.

Owners can expand the system without disruption, with the assurance of a flexible, highly encrypted, permission controlled security system that allows them to focus on growing the business.

Pip Courcoux, Sales and Product Manager - CLIQ Systems for Abloy UK, said: "Lost keys are a serious security risk, but with CLIQ Go it's so easy to manage access control. This revolutionary locking system keeps your business on the move and can be adapted to your organisation's evolving security requirements."

Compatible CLIQ Go products include high security CLIQ cylinders for all door types, which feature a battery in the key for a low maintenance solution, with no cabling and a long lifetime of 200,000 cycles.

CLIQ programming devices are also available for keys, with desktop or mobile versions available. The cloud-based system means that the CLIQ® Go app works seamlessly, and a locksmith can manage the system as an optional service. SST

"Lost keys are a serious security risk, but with CLIQ Go it's so easy to manage access control. This revolutionary locking system keeps your business on the move and can be adapted to your organisation's evolving security requirements."

38 Percent of Organisations in Singapore Rarely Change Security Strategy After a Cyber Attack

CyberArk survey findings show organisations must prioritise securing privileged accounts and credentials in the cloud, on endpoints and across IT environments

Singapore – According to the CyberArk Global Advanced Threat Landscape Report 2018, more than a third (38 percent) of respondents in Singapore stated they rarely change their security strategy substantially – even after experiencing a cyber attack. This level of cyber security inertia puts sensitive data, infrastructure and assets at risk.

Security Starts with Protecting Privileged Accounts

An overwhelming number of respondents in Singapore believe securing an environment starts with protecting privileged accounts – 93 percent stated that IT infrastructure and critical data are not fully protected unless privileged accounts, credentials and secrets are secured.

Singapore respondents named the greatest cyber security threats they currently face, including:

- Ransomware or malware (63 percent)
- Insider threats (60 percent)
- Unsecured privileged accounts (54 percent)
- Targeted phishing attacks (52 percent)
- Unsecured data stored in the cloud (45 percent)

"To build cyber resilience, organisations in Singapore must prioritise what can be done to mitigate threats during an attack in order to effectively protect the company from financial harm and reputational damage," said Vincent Goh, Vice President, Asia Pacific Japan, CyberArk. "Locking down privileged accounts is critical to keeping pace with today's highly skilled threat actors. However, what we see in practice is a rush to invest in 'latest-and-greatest' new security technology; a scattergun approach that lacks the necessary focus on what is truly important to manage and secure."

The Inertia that Could Lead to Data Compromise

The survey findings suggest that security inertia has infiltrated many organisations, with an inability to repel or contain cyber threats – and the risks that this might result in – supported by other findings:

- 36 percent say their organisation can't prevent attackers from breaking into internal networks each time it is attempted
- 34 percent report that administrative credentials were stored in Word or Excel documents on company PCs
- Almost half (47 percent) admit that their customers' privacy or PII (personally identifiable

"To build cyber resilience, organisations in Singapore must prioritise what can be done to mitigate threats during an attack in order to effectively protect the company from financial harm and reputational damage"

information) could be at risk because their data is not secured beyond the legally-required basics

Inertia Towards Securing Credentials and Data in the Cloud Create Cyber Risk

The automated processes inherent in cloud and DevOps mean privileged accounts, credentials and secrets are being created at a prolific rate. If compromised, these can give attackers a crucial jumping-off point to achieve lateral access to sensitive data across networks, data and applications or to use cloud infrastructure for illicit crypto mining activities. Organisations increasingly recognise security in the cloud is a shared burden, and they cannot depend solely on their cloud providers' cyber security. The survey found that:

- More than a third (39 percent) of organisations have no privileged account security strategy for the cloud
- More than half (59 percent) defer on cloud security to their vendor, relying on built-in security capabilities
- 37 percent stated their cloud provider doesn't deliver adequate protection

Changing the Security Culture

To move from cyber security inertia to action necessitates it becoming central to organisational strategy and behaviour, not something that is dictated by competing commercial needs. According to the survey:

- 89 percent of Singapore respondents feel security should be a regular board-level discussion topic
- 47 percent said they recognize or reward employees who help prevent an IT security breach, increasing to nearly three quarters (74 percent) in the U.S.
- Just 9 percent of companies in Singapore continuously perform Red Team exercises to uncover critical vulnerabilities and identify effective responses

"Building awareness of modern cyber security and privacy threats, processes and technologies is just the first step toward an active defence. Companies must show greater urgency to enable cyber security resilience by prioritising cyber security risk at the same level as wider business and financial risks," continued Goh. "Understanding how new technologies - like cloud and DevOps - affect the attack surface is a crucial component of this, as well as the ability to adopt a 'think like an attacker' mindset." SST

Panasonic and Trend Micro Agree to Develop Cyber Security Solution for Connected Cars

Panasonic Corporation and Trend Micro Incorporated, today announced a partnership to jointly develop cyber security solution to detect and prevent cyber-attacks against autonomous and connected cars.

The partnership aims to achieve high security of autonomous and connected cars by developing solution to detect and prevent intrusions into Electronic Control Units (ECUs) that control driving behavior such as acceleration, steering and braking, as well as in-vehicle infotainment (IVI) devices including automotive navigation systems, and telematics*3 devices.

The risks of hackers taking control of steering and braking systems in connected cars are real. New security vulnerabilities are discovered every day and they pose a risk for remote exploitation. It is therefore more important than ever to not only implement security measures in each vehicle but also to analyse new attacks by constantly monitoring in-vehicle systems from the cloud and utilise the results to

> "This partnership will leverage Panasonic's Control Area Network (CAN) intrusion detection and prevention technology and Trend Micro IoT Security. Panasonic's technology will be able to detect any unauthorised commands sent to ECUs that control driving operation, while Trend Micro IoT Security, which utilises Trend Micro's global security intelligence and expertise such as malware analysis, will be implemented on IVI devices such as automotive navigation systems to detect attacks that seek to exploit vulnerabilities through the internet."

implement countermeasures against cyber-attacks to all vehicles.

This partnership will leverage Panasonic's Control Area Network (CAN) intrusion detection and prevention technology and Trend Micro IoT Security. Panasonic's technology will be able to detect any unauthorised commands sent to ECUs that control driving operation, while Trend Micro IoT Security, which utilises Trend Micro's global security intelligence and expertise such as malware analysis, will be implemented on IVI devices such as automotive navigation systems to detect attacks that seek to exploit vulnerabilities through the internet. Through this partnership, events identified by both technologies will be collected and sent to an analysis platform in the cloud to detect and block suspicious traffic.

The overall development will enable the provision of solution including in-vehicle and cloud systems to prevent cyber-attacks against autonomous and connected cars. Panasonic and Trend Micro will be working jointly on the development and aim to launch commercially after 2020.

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

MIT and SenseTime Announce Effort to Advance Artificial Intelligence Research

Alliance will be part of new MIT Intelligence Quest

MIT and SenseTime today announced that SenseTime, a leading artificial intelligence (AI) company, is joining MIT's efforts to define the next frontier of human and machine intelligence.

SenseTime was founded by MIT alumnus Xiao'ou Tang PhD '96 and specialises in computer vision and deep learning technologies. The MIT-SenseTime Alliance on Artificial Intelligence aims to open up new avenues of discovery across MIT in areas such as computer vision, human-intelligence-inspired algorithms, medical imaging, and robotics; drive technological breakthroughs in AI that have the potential to confront some of the world's greatest challenges; and empower MIT faculty and students to pursue interdisciplinary projects at the vanguard of intelligence research.

SenseTime is the first company to join a new Institute-wide initiative, the MIT Intelligence Quest, since its launch earlier this month. The MIT Intelligence Quest seeks to leverage the Institute's strengths in brain and cognitive science and computer science to advance research into human and machine intelligence in service to all humanity. It will apply the fruits of its discoveries to diverse fields — from materials design to finance to early disease diagnosis — while considering deeply the economic, cultural, and ethical implications of AI.

An essential element of the new initiative is forging connections with innovative companies and individuals who share MIT's passion for work in intelligence.

"As an MIT alumnus, I'm grateful to have this opportunity to collaborate with my alma mater, especially on something that is dear to my heart — to advance research on artificial intelligence," says Tang, who is also a professor of information engineering at the Chinese University of Hong Kong. "SenseTime is committed to innovating in the fields of computer vision and deep learning. With the creation of the MIT-SenseTime Alliance on Artificial Intelligence, I'm confident that we will bring together the world's best and brightest talent to further advance the state of the art for AI to the benefit of society."

Li Xu, CEO and co-founder of SenseTime, adds, "MIT has long been at the forefront of research into artificial intelligence. As the largest provider of AI algorithms in China, SenseTime has worked with more than 400 leading customers and partners to solve hard, real-world problems. We are very excited to join hands with MIT to lead global AI research into the next frontier."

The alliance emerges from a longstanding connection between MIT and Tang, who conducted his PhD research in underwater robotics and computer vision at the Institute more than 25 years ago, applying computer vision to the study and classification of underwater imagery. One of his advisors was W. Eric L. Grimson PhD '80, now the chancellor for academic advancement at MIT and the Bernard M. Gordon Professor of Medical Engineering.

"Considered China's leading AI "unicorn" valued at more than $3 billion, SenseTime has developed a sophisticated proprietary deep learning platform and built applications for multiple industries. The company has applied its core computer vision technologies, including face recognition, video analysis, text recognition, and autonomous driving, across industries such as automobile, finance, mobile Internet, robotics, security, and smartphones."

"Xiao'ou has used the same practical approach to computation and artificial intelligence that he displayed at MIT to build a highly successful academic and applied research career and a tremendously successful, technologically impressive startup company in SenseTime," Grimson says. "He has become well known throughout China and the world as a leader in the field of AI, and especially computer vision and deep learning. Xiao'ou has always kept MIT front of mind, both as a professor and an entrepreneur. He has shared intellectual ideas and is ever on the lookout for impressive young talent whom he encourages to apply to the Institute. I personally am proud of Xiao'ou's success and the impact he is making on the world, and look forward to a deepened, mutually beneficial relationship between MIT and SenseTime."

Anantha P. Chandrakasan, dean of the MIT School of Engineering and the Vannevar Bush Professor of Electrical Engineering and Computer Science, who recently helped to lead the development of the MIT Intelligence Quest, says, "I am thrilled that SenseTime has chosen to join us as we embark on our quest to achieve a deeper understanding of the science and engineering of intelligence and to harness that understanding to create a better world. Dr. Tang is no stranger to innovative research, and the MIT-SenseTime Alliance on Artificial Intelligence will facilitate boundary-pushing research in intelligence across the Institute and give faculty and students opportunities to unlock new thinking through intense collaboration. This is an exciting moment for both MIT and SenseTime."

MIT has been on the frontier of intelligence research since the 1950s, when pioneers Marvin Minsky and John McCarthy helped establish the field of artificial intelligence. MIT pushed several major advances in the subsequent decades from neural networks to data encryption to quantum computing to crowdsourcing and the Institute now has more than 200 principal investigators whose research bears directly on intelligence. Currently, the Computer Science and Artificial Intelligence Laboratory, MIT Media Lab, Department of Brain and Cognitive Sciences, Center for Brains, Minds and Machines, and MIT Institute for Data, Systems, and Society serve as connected hubs for AI and related research at MIT.

Considered China's leading AI "unicorn" valued at more than $3 billion, SenseTime has developed a sophisticated proprietary deep learning platform and built applications for multiple industries. The company has applied its core computer vision technologies, including face recognition, video analysis, text recognition, and autonomous driving, across industries such as automobile, finance, mobile Internet, robotics, security, and smartphones.

SenseTime is currently working on developing autonomous driving, intelligent medical treatment, and deep learning hardware optimisation. It is also strengthening its technology platform and attracting leading talent from around the world to open up greater applications scenarios and a SenseTime-driven AI commercial ecosystem. The company has offices in Beijing, Chengdu, Hangzhou, Hong Kong, Kyoto, Shanghai, Shenzhen, Singapore, and Tokyo. SST

Move into the Age of Digital Parenting with the Omate x Nanoblock Smartwatch for Children

Omate selects Tata Communications to launch its Omate x Nanoblock smartwatch for children with instant, secure, global connectivity

Tata Communications, a leading digital infrastructure provider, and wearables maker Omate are working together to equip the new Omate x Nanoblock children's smartwatch with instant, secure, global connectivity straight out of the box. With a Tata Communications MOVE - IoT Connect™ SIM built in, the Omate x Nanoblock will pave the way towards a new frontier of digital parenting.

Smartwatches such as the Omate x Nanoblock help parents stay connected with their children and know exactly where they are when needed – providing invaluable peace of mind. This peace of mind is now reinforced in the Omate x Nanoblock because Tata Communications MOVE - IoT Connect™ carries all location, messaging and video calling data over an end-to-end encrypted virtual private network (VPN), ensuring maximum security.

"Given the growing threat of cyber- crime, any device or application aimed at children must be safeguarded with the highest levels of security," said Laurent Le Pen, Founder & CEO, Omate. "What sets the Omate x Nanoblock apart from other children's smartwatches is the extra security layer provided by the global private network of Tata Communications MOVE – IoT Connect™. It means that parents can keep track of and in touch with their kids in real-time, but no data on the network can be intercepted by unscrupulous individuals."

Tata Communications MOVE – IoT Connect™ harnesses Tata Communications' relationships with more than 600 mobile network operators (MNO) around the world to bring the Omate x Nanoblock reliable, high-quality network connectivity anywhere in the world. These relationships also help accelerate Omate's international expansion outside its home market in China, allowing the company to sell the smartwatch to retailers and other partners as a 'wearable-as-a-service', eliminating the need for separate data connectivity agreements with different local MNOs in each country.

"IoT Connect™ platform is fully integrated with Omate's business processes, giving the company real-time visibility over customers' data usage patterns, and control over tariffs and billing. This means that when a new customer switches on the smartwatch for the first time, it is instantly connected. The software-defined capabilities of Tata Communications MOVE – IoT Connect™ also make it easy for Omate to customise features and content with children's needs in mind. "

"The immense transformational potential of the Internet of Things hasn't been unlocked yet because the mobile networks which these applications depend on are inherently local," said Anthony Bartolo, Chief Product Officer, "Yet, businesses like Omate that want to reach customers worldwide, need truly global, borderless connectivity to power their IoT devices and applications. They can't be constrained by local MNOs' roaming policies. Through our partnerships and the ubiquitous network of Tata Communications MOVE – IoT Connect™, businesses are able to capture, move and manage information on a global scale, and give people the always-connected digital experiences they crave."

The API-enabled, automated Tata Communications MOVE – IoT Connect™ platform is fully integrated with Omate's business processes, giving the company real-time visibility over customers' data usage patterns, and control over tariffs and billing. This means that when a new customer switches on the smartwatch for the first time, it is instantly connected. The software-defined capabilities of Tata Communications MOVE – IoT Connect™ also make it easy for Omate to customise features and content with children's needs in mind.

Laurent Le Pen continued stating "the completely automated subscriber and connectivity management capabilities of Tata Communications MOVE – IoT Connect™ allow us to focus on our core business of developing innovative, feature-rich smart watches for consumers everywhere. As we set our sights on taking on some of the biggest consumer electronics manufacturers in the world, working with Tata Communications gives us the global reach we need to help drive the growth of our business across Asia, Europe and the Americas." SST

Dahua Smart IoT Industrial Park Brings Productivity and Quality to a New Level

To grasp the current manufacturing trends and seize the Zeitgeist of Industry 4.0, a new smart IoT industrial park in Hangzhou has been put to use in June, 2017 by Dahua Technology, a leading solution provider in the global video surveillance industry.

Dahua Smart (IoT) Industrial Park occupies in total 512 acres in Fuyang district of Hangzhou, about20 minutes' drive from Dahua headquarters, designed to host 6000 staff (by 2017, 4500 people have been working/ living in the 262 acres of phase one area). With topnotch technologies, personnel, materials and other benefits, Dahua's smart industrial park will bring productivity and quality to a brand new level.

Dahua Smart IoT Industrial Park

Faster Production and Adaption

The automatic production solution based on integrated information system not only grants a higher productivity that significantly shortens the delivery cycle time for Dahua customers, but also a greater flexibility to specialised requests and ever-changing reality.

The employment of software such as ERP, PLM, PDM, MES, APS and WMS helps to achieve information integration, which, combined with industrial cameras, RFID sensory technologies and automation technologies, can integrate personnel, logistics, works, engineering projects and finance from respective sections of production(preparation, assembly,

> "The faster speed also applies to the development of new molding, since Dahua smart industrial park provides the great benefit of internal synergy, allowing the end-to-end vertical supply chain with marketing, R&D and manufacturing efficiently integrated."

testing, packaging, inspection, shipment), rendering the whole process visible, traceable and digital.

The mounter serves as a good synecdoche to illustrate the incredible efficiency of the whole production system. The concerning high-end devices (including mounter, printer, automated optical inspection equipment, Ersa reflow soldering tools, etc) provided by ASM (originally Siemens) achieve a speed among the fastest in the world. According to IPC standard, X4iS, the latest high-speed mounter can process 125,000 components per hour, or 35 per second. X35 multifunctional mounter can do 54000 components per hour, or 15 per second. A production line in X series can enhance the productivity by 2.7 times while reducing the consumption of energy by 52%, comparing to the original production line in D series under the same conditions.

The faster speed also applies to the development of new molding, since Dahua smart industrial park provides the great benefit of internal synergy, allowing the end-to-end vertical supply chain with marketing, R&D and manufacturing efficiently integrated. The advanced organizing system is supported by topnotch equipment, such as MAKINO high-speed graphite processing machine, GF CNC, GF WEDM-LS machine, Hexagon 3D Nikon projectors and electronic displays. With a processing accuracy of +/-0.002 to +/-0.005MM, while also supporting CAD / CAM / CAE collaborative development and simultaneous manufacturing, these machines enable Dahua to develop new mechanical molding in as short as 7 days.

By far, this developing system has already produced high precision molding for Lechange Robots, monitoring cameras in TP1-TC6 series, G20 intelligent head-gears, smoke alarm for fire detectors, etc., all of which proving the effectiveness of the system in shortening the development cycle and keeping the competitive edge with new products in the business.

> "Higher quality saves lots of time and economic costs for clients. Even more importantly, higher quality results in less likelihood for products to malfunction especially when they are used in critical, not-allowed-to-go-wrong situations."

Higher Quality

Higher quality saves lots of time and economic costs for clients. Even more importantly, higher quality results in less likelihood for products to malfunction especially when they are used in critical, not-allowed-to-go-wrong situations. Dahua's products are guaranteed with a higher quality for two reasons: first, Dahua has set a high standard of accuracy in production; second, with a reliability lab at the production end, Dahua has put together an effectively closed loop for quality control in the manufacturing process.

Accuracy Enhanced

Accuracy has always been one vital index defining the manufacturing ability because it directly sets the limit to quality and range of products to be produced. Again, take the mounter mentioned above for example: it can process components, in metric size, as small as 03015(0.3x0.15mm), with a +-0.025mm SMD precision (within the 3-stigma range), boasting world leading performance and capable of covering basically all types of components used in the industry.

Dahua industrial camera plays an important role in IoT, providing a closed loop for quality control in the manufacturing process, in which all materials, personnel and devices are connected and products are traceable to the specific production line and precise time it got made. Boasting a variety of functions, Dahua industrial cameras are used in different sections of production, enabling automatic assembly, high-precision graphic inspection and product flaw inspection. Through high definition machine vision, Dahua industrial cameras automatically and precisely locate the components, limiting the assembly error to micron level. Equipped with enhanced vision and intelligent analytics algorithm, the industrial camera can spontaneously detect and recognize flaws in the performance and outlook of products, thus promising not only the volume of cameras production but also the steady quality of each and every one of them.

Reliability Reinforced

Reliability must be put to test, in R&D as well as in manufacturing process. The reliability lab at the production end serves to assure quality by randomly taking products from production lines and put them into reliability tests simulating falling, high/low temperature, worn-out conditions, which are conducted by industry leading testing equipment in the lab. Thus what's conceived in R&D is confirmed from the production line, the synergy of both ends promising better products (for common use or specialised needs). This lab is also responsible for testing all the raw materials. Thanks to the aforementioned information integration, all tests are automatically conducted, recorded and traceable.

In conclusion, Dahua Smart (IoT) Industrial Park is endowed with the latest and world leading manufacturing equipment/system boasting high level automation and intelligence, which is essential to satisfy the ever higher demands from clients in terms of delivery time, specialised use and quality. There is still great potential to this new smart industrial park. It is literally only in its phase one. And in the future phase, it is expected to be more intelligent, to realise client-centered flexible production and to enable a safer society and smarter living. SST

Dimension Data Enables A Leading Global Professional Services Firm To Modernise Its New 'Smart Campus' In Hyderabad With Software Defined Access

The Smart Campus, among other things, will be IoT enabled with smart lighting and smart parking

Dimension Data, the global ICT solutions and services provider, today announced its strategic partnership with a leading global professional services firm to modernise its IT infrastructure for their new Smart Campus in Hyderabad. The smart campus will be IoT enabled with smart lighting and smart parking. Dimension Data has upgraded the firm's IT infrastructure with Software Defined Access (SD-access), which enables automated end-to-end segmentation to separate user, device and application without redesigning the network.

Through Software Defined Access, Dimension Data has enabled the firm to have seamless user mobility within the campus and between campuses. SD-access allows the client to create policy compliance to create an agile IT infrastructure to support faster launch of business services, and consistency to a large disparate network, improving resolution times. The upgraded system also provides higher Power over Ethernet (PoE) to enable smart sensors.

The India software defined networking market is forecast to grow at a CAGR of 36% during 2017 – 2022, according to Research and Markets. Increasing need among organisations for agile and efficient networking infrastructure, which can be monitored and managed centrally is driving this growth. The current network infrastructure needs to support myriad digital initiatives that can include expanded enterprise mobility programs, Internet of Things (IoT), and increased internal application development, all at scale. These efforts are taking place against a backdrop of explosive data growth and a growing, more sophisticated security threat landscape.

"The smart campus will be IoT enabled with smart lighting and smart parking. Dimension Data has upgraded the firm's IT infrastructure with Software Defined Access (SD-access), which enables automated end-to-end segmentation to separate user, device and application without redesigning the network."

"There was an impending need for the firm to move away from traditional network architecture that demanded higher manual intervention and does not support automation. Dimension Data's implementation of SD-access has ensured the seamless convergence of people, technology and workplace to improve agility, productivity and engagement for the firm. The solution will provide a secure and seamless mobile experience to the user, thereby increasing productivity and flexibility, the core of a Digital Workplace," said KN Murali, Solutions Head, Dimension Data India. SST

Off-the-Shelf Smart Devices Found Easy to Hack

Ben-Gurion University Researchers Offer Cyber-Safety Tips to Protect Cameras, Baby Monitors, Doorbells, and other IoT Devices

Off-the-shelf devices that include baby monitors, home security cameras, doorbells, and thermostats were easily co-opted by cyber researchers at Ben-Gurion University of the Negev (BGU). As part of their ongoing research into detecting vulnerabilities of devices and networks expanding in the smart home and Internet of Things (IoT), the researchers disassembled and reverse engineered many common devices and quickly uncovered serious security issues.

"It is truly frightening how easily a criminal, voyeur or pedophile can take over these devices," says Dr. Yossi Oren, a senior lecturer in BGU's Department of Software and Information Systems Engineering and head of the Implementation Security and Side-Channel Attacks Lab at Cyber@BGU. "Using these devices in our lab, we were able to play loud music through a baby monitor, turn off a thermostat and turn on a camera remotely, much to the concern of our researchers who themselves use these products."

"It only took 30 minutes to find passwords for most of the devices and some of them were found only through a Google search of the brand," says Omer Shwartz, a Ph.D. student and member of Dr. Oren's lab. "Once hackers can access an IoT device, like a camera, they can create an entire network of these camera models controlled remotely."

The BGU researchers discovered several ways hackers can take advantage of poorly secured devices. They discovered that similar products under different brands share the same common default passwords. Consumers and businesses rarely change device passwords when purchased so they could be operating infected with malicious code for years.

They were also able to logon to entire Wi-Fi networks simply by retrieving the password stored in a device to gain network access.

Dr. Oren urges manufacturers to stop using easy, hard-coded passwords, to disable remote access capabilities, and to make it harder to get information from shared ports, like an audio jack which was proven vulnerable in other studies by Cyber@BGU researchers. "It seems getting IoT products to market at an attractive price is often more important than securing them properly," he says.

Tips for IoT Product Security

With the goal of making consumers

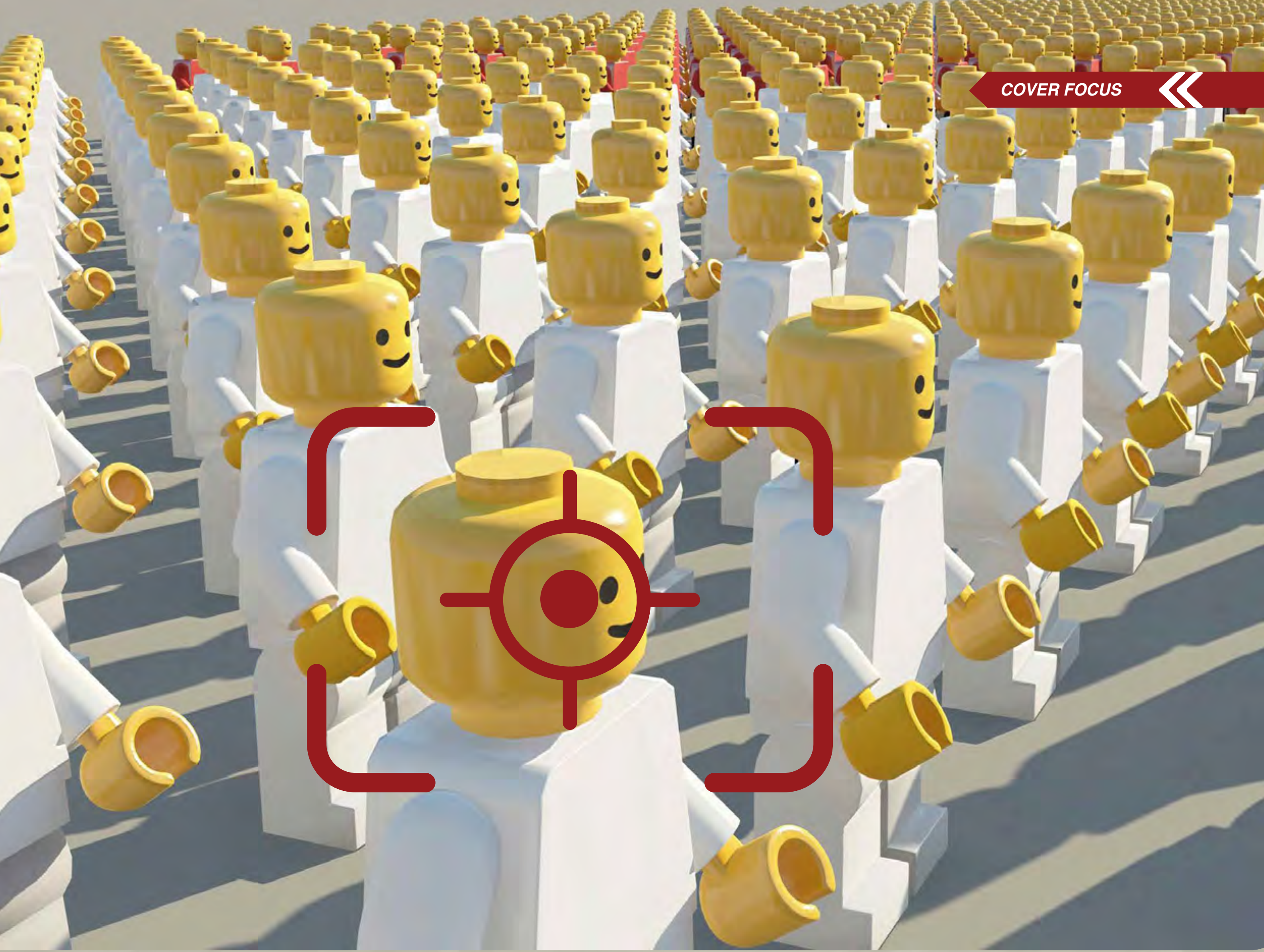
smarter about smart home device protection, BGU researchers offer a number of tips to keep IoT devices, families and businesses more secure:

- Buy IoT devices only from reputable manufacturers and vendors
- Avoid used IoT devices. They could already have malware installed
- Research each device online to determine if it has a default password and if so change before installing
- Use strong passwords with a minimum of 16 letters. These are hard to crack
- Multiple devices shouldn't share the same passwords
- Update software regularly which you will only get from reputable manufacturers
- Carefully consider the benefits and risks of connecting a device to the internet

"The increase in IoT technology popularity holds many benefits, but this surge of new, innovative and cheap devices reveals complex security and privacy challenges," says Yael Mathov, who also participated in the research. "We hope our findings will hold manufacturers more accountable and help alert both manufacturers and consumers to the dangers inherent in the widespread use of unsecured IoT devices."

"The BGU researchers discovered several ways hackers can take advantage of poorly secured devices. They discovered that similar products under different brands share the same common default passwords. Consumers and businesses rarely change device passwords when purchased so they could be operating infected with malicious code for years."

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



THE MODERN AND INTELLIGENT CCTV

►► *By Vlado Damjanovski, CEO of ViDi Labs, www.vidilabs.com*

The digital (r)evolution of the last twenty years changed almost everything. Analogue vinyl records morphed into CDs with MP3 formats; rotary dialed telephones became digital wireless mobile devices; celluloid films and movies became digital solid state sensor produced movies displayed on huge LCD or OLED screens, the whole world got connected on so many different levels via Internet.

In the security industry, the Closed Circuit Television (CCTV) technology migrated from the old analogue PAL/NTSC based cameras with limited resolution of 480TV lines into digital IP cameras with incredible resolution and almost limitless recording capacity. The HD television standard increased the analogue resolution five fold, and the latest UHD (aka 4k) offers an incredible ten times the details of analogue CCTV.

When all of the above is converted into data - it is an amazing amount of data.

For example, just one hour of 4k video, uncompressed, would occupy around 2TB of storage! As we all know, in CCTV we always record multiple cameras, and much longer recordings are required, so we have no choice but to compress. Most common video compressions are H.264 and H.265, which allow for multi-camera system recording of one week, two weeks or even a month by a CCTV system. So, for example, a 4k-compressed video stream of 10Mb/s for one hour will occupy around 5GB of data space. A small 16-camera system for one week of recording will take around 12TB, and for one month around 50TB. This is achieved easily with 5 x 10TB drives on one server today.

So, in short, long storage of IP CCTV cameras today is no longer a problem.

The real challenge we are faced with is how quickly and efficiently an incident can be responded to, in a 'pro-active' designed system, that is - a system with 24hrs operation. In a non-manned system 'reactive' CCTV system, we rely on the incident being found after the fact. So, the real challenge today is - if we have one month of recording, how quickly can we find such an incident?
If the security operator doesn't knows at what time and on what camera the incident occurred, he/she will have a tough task to find it in a 30 days of recording. Even if the operator decides to do a fast playback - it will still take a considerable amount of time, and frankly, nobody wants to do this.

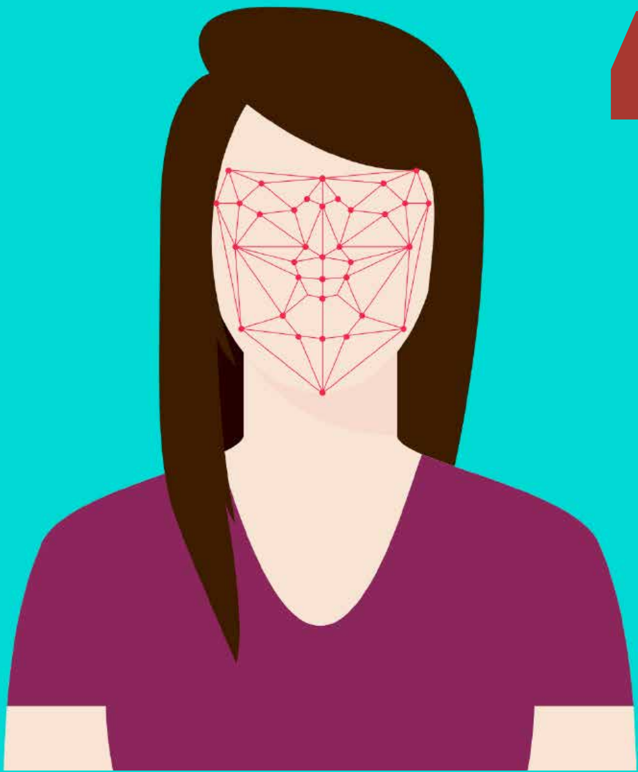
Luckily, with the advancement of faster computers, more intelligent software, and the introduction of deep learning concepts we are at a point in our evolution as technology where many companies offer a real helping hand to the above mentioned problems.

This is usually referred to us Video Contents Analytics (VCA). The IEC standards Technical Committee TC-79 are in fact working on it right now.
An incident that happened in the past 30 days, as long as it can be described with some basic data, can be found very quickly by simply running a VCA routine in the background of a server. This could be in the form of 'smart search' or 'appearance' or 'disappearance' of an object. For example, an object has been left unattended at the airport for longer than 5 minutes, or perhaps an expensive painting disappeared from an exhibition hall. Automatic identification of faces 'on the fly' today is reasonably easy to do.

Hundreds of people being picked up by one or more cameras can immediately be identified and logged into a database, which can then compare those faces with black- listed (not allowed) or white-listed (allowed) faces. This can be used, for example, in a casino to warn the security staff of a VIP, or perhaps a banned gambler. Such a system can even be used to operate access control system, which is in a way what the iPhone X is doing today.

Some advanced VCA software offers the so called heat-maps, by indicating with different colors which area in a shopping centre for example, are visited by more

> ***An incident that happened in the past 30 days, as long as it can be described with some basic data, can be found very quickly by simply running a VCA routine in the background of a server. This could be in the form of 'smart search' or 'appearance' or 'disappearance' of an object. For example, an object has been left unattended at the airport for longer than 5 minutes, or perhaps an expensive painting disappeared from an exhibition hall. Automatic identification of faces 'on the fly' today is reasonably easy to do.***



> ***With the modern VCA it is possible to ask a CCTV system to find all people in red shirt in the past 30 days, for example, walking on a particular street and in a particular direction. Furthermore, some systems can even discern if the people being analysed are male or female, and even guess an approximate age of a person based on the video footage. So, it won't be very difficult to enter the following search criteria: "find me a young Caucasian male, aged between 25 and 35, wearing blue shirt, in the last 30 days.***

people, and which are less visited. Suddenly this VCA can also be used as a marketing analysis tool. It is also possible using VCA to determine loitering in an area, or perhaps have the CCTV warn operators if there is a fight starting in a street mall.

Another VCA example is vehicle flow data, by showing which exit or entry at a big roundabout for example, is the busiest and at what time of the day. You can easily search by colour and/or vehicle type. A great tool to help traffic authority reduce traffic congestions. Searching for example for a red car that went to the south of the city in the past week, is easily done.

An automatic vehicle number plate recognition has been successfully done now for quite a few years. Vehicles speeding even up to 250km/h can be picked up and identified. Furthermore, it is possible to determine the vehicle speed via the video, no speed radars needed. This helps, again, in traffic analysis, traffic light operation, capturing offending speeding cars, etc. Finding where an offending vehicle was on a certain day using an automated number-plate detection could be a breeze.

Some companies offer intelligent VCA to casinos for example, by statistical analysis of each gambler, on each table, by knowing their chips, cards, analysing their strategy, and thus predicting the possibility of unfair gambling where the casino may loose considerable amount of money. The casino VCA may be of great assistance here.

With the modern VCA it is possible to ask a CCTV system to find all people in red shirt in the past 30 days, for example, walking on a particular street and in a particular direction. Furthermore, some systems can even discern if the people

being analysed are male or female, and even guess an approximate age of a person based on the video footage. So, it won't be very difficult to enter the following search criteria: "find me a young Caucasian male, aged between 25 and 35, wearing blue shirt, in the last 30 days." Also instead of playing every single camera for the past 30 days, let the VCA do the work, and in a few seconds or minutes, come up with a number of possibilities which the operator then can view, further analyse and make his/her decision about the potential culprit.

One interesting strategy that help VCA being further and quicker improved is that there are VCA companies that specialise in only one thing: either license plates recognition (LPR), or face identification (FI), or traffic analysis, instead of having each and separate CCTV system manufacturer develop their own LPR, FI, or other VCA. Then, such highly developed package is sold to various VMS manufacturers to be added into their system and become one intelligent complete VMS. In a way, such VCA modules become like an app within a VMS system.

This, in my opinion, is the correct way and offers quicker evolution to a mature VCA, which helps the security operators much quicker and better to what was the case earlier in our industry.

In all of the above-described VCA scenarios, one basic pre-condition is of the utmost importance for successful analytics: The IP CCTV cameras have to have good sensors and good optics. But more importantly, the camera and lens setup at the installation time has to be appropriate in order to offer sufficient details for the analysis.

You cannot read the vehicle number plate even with the best LPR software, if the camera has a long electronic exposure, or the lens angle of view is too wide as to read the number plates.

Similarly, you will not be able to identify faces, if the camera/lens combination does not give you sufficient pixel details and the same goes for casino applications, in banks for recognising money, etc.
The IP CCTV industry has advanced tremendously in the last 10 years, but it is now even more important to understand the limitations of lens quality and video compression, and how them up to have the best possible video footage for further automated analysis.

Although there are many things that can be discussed further, there are tools, which can be used as an aid in camera setups. One such tool is the ViDi Labs SD/HD test chart, and especially the 'ViDiLabs calc' app.

The 'ViDiLabs calc' can be used across all VCA scenarios, by just simply knowing the required pixel density for the given analysis. By knowing the camera parameters it is very easy to calculate the optimal settings for successful VCA analysis.

To find out more about this, search on iTunes for 'ViDiLabs calc'. SST

About the Author:
Vlado Damjanovski is a renowned CCTV authority based in Australia. He is a published author of four books on CCTV, translated in Russian, Korean and German languages. He regularly visits Singapore to conduct seminars based on his books (www.cctvseminars.com) and to present various technology topics. A new visit is planned for August 2018, and all interested to attend his presentation can contact him at vlado@vidilabs.com

Chester Zoo Uses IP Video to Maximise Security and Operational Efficiency

Background

Chester Zoo has grown rapidly since its foundation in 1930 so that today it is spread across more than 125 acres, housing more than 15,000 animals and 500 different species. It attracts more than 1.9 million visitors each year - making it the most popular UK visitor attraction outside London. With further growth planned, Chester Zoo began a site-wide vulnerability assessment, led by the zoo's then head of security, Nigel Peers, out of which flowed a series of recommendations for modernisation of the Zoo's security.

Requirements

The Zoo needed a fully-integrated and networked camera system to enable the security team to spot and act on all threats faster; tighten perimeter security; improve visitor and staff health and safety monitoring; and support keepers in assuring the welfare of the animals in their charge. The new system needed to be centralised to support the fully-professionalised security patrolling team. However, video also needed to be distributed effectively to enable health and safety officers, keepers and researchers, to view specific sets of camera images when necessary. All this was only possible working in close partnership with IP video specialist systems integrator NW Systems Group.

Solution

Improving image quality and coverage

NW Systems, once on site, initially discovered that many of the legacy CCTV cameras were generating poor images. NW Systems replaced approximately 60 faulty CCTV cameras with new Axis network cameras. Meanwhile, all remaining CCTV cameras were networked using Axis M7016 and M7014 Encoders, alongside

all new network camera transmissions. A total of 160 new Axis cameras were installed and networked by NW Systems across the original or 'core' zoo, The Islands and elsewhere, together providing much more comprehensive coverage site-wide. Axis P3225-LVE cameras were installed in numbers across The Islands, partly because of their versatility and robustness making it possible to site them both inside and outside animal enclosures.

Special attention was paid to siting of cameras for total discretion. Where surroundings required, camera housings were camouflaged, thereby offering highly unobtrusive surveillance. In addition, the newly centralised control room was fitted with the very latest video management software (VMS) from Milestone Systems.

Supporting animal welfare and keeper safety needs in the Elephant enclosure

NW Systems was also called in to help solve a specific concern of the Zoo's Lead Elephant Keeper, associated with opening large gates to let the elephants out of the Elephant House into the wide-open habitat and back into the elephant house at night.

The existing remote door control system was enhanced by high quality live views provided by five-megapixel Axis P1357-E network cameras covering the doors. These same cameras were also being used to capture the magical moments of elephants giving birth to their babies – three baby elephants have been captured on these cameras over the last 18-months. The video sequences were shown live via the Zoo's website and recordings have also been kept for marketing purposes.

"Chester Zoo now has a video security platform which is highly reliable, expandable and future-proof. We know that whatever our requirement in terms of intelligence, video analytics and integration with other physical security systems such as intruder alarms or access control systems; it's possible to bring it all together with our new IP video system displayed in the Zoo's new security control room. Speed and appropriateness of response to threats is now assured."

-Nigel Peers, Security Manager, Chester Zoo

In the city of Jinan, officials use cameras *to identify and publicly shame jaywalkers. Photos of offenders caught in the act are shown on a screen next to crosswalks, along with personal information about the person, like their home address and ID number.*

The Temple Of Heaven Park in Beijing *is using facial-recognition technology to dole out short strips of toilet paper in a high-tech experiment to wipe out thieves. Equipped with facial recognition software, the machine hands out about two feet of tissue to combat the park's problem of thieves stealing 30 rolls of toilet paper from park restrooms on a daily basis.*

SURVEILLANCE THE CHINA WAY

A SNEAK PEEK INTO CHINA'S CREATIVE USAGE OF CCTV

At Megvii, marketing manager Zhang Xin boasts *that the company's Face++ program helped police arrest 4,000 people since the start of 2016, including about 1,000 in Hangzhou, where a major deployment of cameras in hotels, subways and train stations preceded that year's G-20 summit.*

Facial recognition cameras allow access *to residences. A 40 year old housewife commented that she no longer has to deal with the hassle of opening doors when she has her hands full because a mere glance at the CCTV will open her apartment door.*

Street cameras automatically classify *passers-by according to gender, clothes and even hair length, and software allows people to be tracked from one surveillance camera to the next, by their faces alone. Gradually, a model of people's behaviour takes shape. Once a criminal or a suspect is identified, their connections with other people can be looked at and If another person has multiple connections, they also become suspicious. Profiling through surveillance.*

In Zhengzhou, Chinese police *are now using sunglasses with inbuilt facial recognition software for surveillance purposes. The glasses were tested at train stations where they were used to scan travellers during the Lunar New Year migration. This is an extremely busy period of holiday travel, often described as the largest human migration event on Earth and police said the sunglasses had already been used to capture seven suspects wanted in major cases, as well as 26 individuals traveling under false identities.*

Hotels, schools and kindergartens *are installing cameras to scan people's faces before allowing entry. Some colleges have even resorted to installing this technology to spot "ghost writers" trying to sit exams for other students and one KFC in Beijing is scanning customers' faces to recommend menu items based on factors including age, gender and mood. Facial recognition technology will be expanded to KFC's 5,000 stores around China and potentially normalised into other public-facing services.*

The Sharp Eyes project *which is the Chinese government's plan to make an omnipresent video surveillance network to track where people are and what they're up to, aims to mobilise neighborhood committees and snoopy residents who have long been key informers. Now, state media reports, some can turn on their televisions or mobile phones to see security camera footage, and report any suspicious activity such as a car without a license plate, an argument turning violent, directly to the police.*

Tightened security at main entrance and car park

NW Systems also provided increased coverage across the recently renovated Jubilee Quarter, the Zoo's main entrance and large car park serving it. It installed several Axis Q6000-E PTZ Dome Network Cameras, alongside Axis C3003-E Outdoor Network Horn Speakers, clamped onto existing lighting masts throughout the car park. This enables the Zoo's security team to monitor activity around the 1000-vehicle capacity car park, for the protection of visitors and their belongings. The loud speakers can be used to transmit live messages to arriving visitors to guide them towards the entrance and to deter any potential wrong-doing.

Results

Over a three-year period, working in close partnership with the UK's largest visitor attraction outside London and largest zoo in the UK, NW Systems has helped Chester Zoo to rationalise, network and centralise its security operation. The result is a state-of-the-art IP camera system which transmits video from nearly 300 Axis cameras to a modern, IP-based control room.

The new system has underpinned the professionalisation of the Zoo's security team. It has also provided the right platform for distribution of high quality video images to meet zoo keepers' specific operational needs, including animal welfare and behaviour research requirements. The Zoo's security team can now identify potential threats more rapidly using video images to brief patrolling officers on where to go and what to anticipate on arrival - live and recorded video can even be delivered to patrolling officers' mobile devices on the ground. The system enables the security team to spot and discourage inappropriate visitor interaction with animals, and record vital evidence in case of any incidents which might result in insurance claims.

Following-up events and evidence gathering has also been improved - including supplying timely, high quality video footage to the Police when necessary. Vanderbilt networked intruder alarms have also been installed by NW Systems to further protect key buildings around the site.

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

> "I'm very proud that we've been able to work with Chester Zoo every step of their three-year journey to upgrade and harden their physical security provision; while also creating a camera system which supports many other operational requirements from visitor and staff health and safety, to animal welfare and behaviour research, as well as retail management and loss prevention."
>
> ***-Frank Crouwel, Managing Director, NW Systems***

Cybersecurity for Smart Buildings

Cyberbit provides cyber security solutions for smart buildings, including the Ram Compound, which is the first smart-building government facility in Israel, and considered to be one of the most innovative IT projects in the country. Smart buildings use automated processes to control the building's operational systems and increase reliability and efficiency. The Ram Compound will serve as headquarters for sensitive government ministries and as such integrates physical and cybersecurity to achieve resilience.

Cybersecurity Challenges

Automation and digital control provide functional and operational advantages, but also introduce new cybersecurity risks:

Tampering with surveillance systems – attackers can now put

> "Attackers are always looking for the weakest link to exploit,so security must be implemented seamlessly across both the IT and OT networks. We selected Cyberbit due to the technical superiority of its portfolio and ability to provide integrated, end-to-end cyber security across the entire IT/OT stack."
>
> ***-Lior Kalev, Information Security Expert and Head of Cyber Risk Services , Deloitte***

surveillance systems out of service or take control of them.

Putting critical physical systems out of service – attackers can access and damage elevator control systems, gates, or the entire power system.

Taking control of IP connected devices – attackers may take control of connected devices such as cameras to retrieve sensitive data or to use as an internal attack vector, as in the case of the DYN attack.These challenges join the array of existing IT security risks, such as compromising sensitive data and disruptions to business continuity.

Project Goals

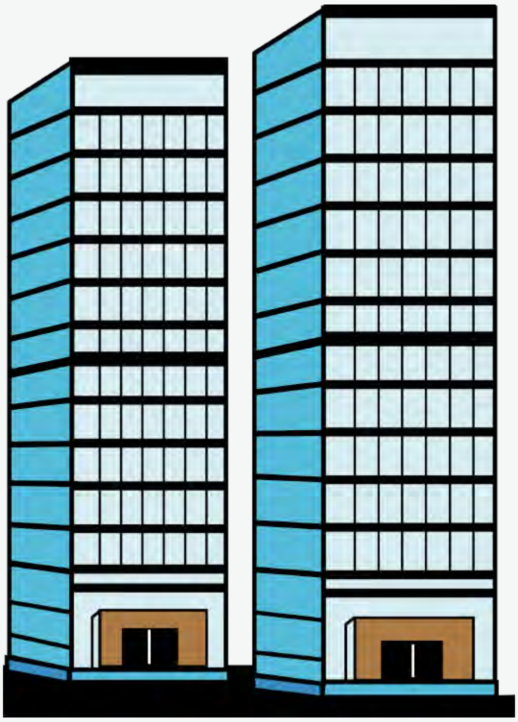
The Israeli government defined cyber resilience as a primary goal of the Smart Building project. The typical goals of a smart building project such as the Ram Compound are:

Integrated security across the entire infrastructure

The solution must secure the entire IT, OT and IoT infrastructure and devices, and should analyze data from all 3 segments to understand context rapidly in the event of a multi-vector attack, or when an attacker moves between segments.

Centralised visibility

The building's security operations are managed centrally, at a Security Operations Center (SOC). SOC managers and analysts must have 24/7 situational awareness across IT, OT and IoT segments and have access to data, dashboards and reports, which visualise security systems in a central location, and provide cross-segment information and context in the event of an IT/OT attack.



Centralised incident response

In the event of a security incident, the SOC team will manage it centrally, at the SOC. This requires access to all security tools from a single location, as well as access to data from all systems and segments in real-time, to investigate it during the incident

Project Goals

The Israeli government defined cyber resilience as a primary goal of the Smart Building project. The typical goals of a smart building project such as the Ram Compound are:

Integrated security across the entire infrastructure

The solution must secure the entire IT, OT and IoT infrastructure and devices, and should analyse data from all 3 segments to understand context rapidly in the event of a multi-vector attack, or when an attacker moves between segments.

Centralised visibility

The building's security operations are managed centrally, at a Security Operations Center (SOC). SOC managers and analysts must have 24/7 situational awareness across IT, OT and IoT segments and have access to data, dashboards and reports, which visualise security systems in a central location, and provide cross-segment information and context in the event of an IT/OT attack.

Centralised incident response

In the event of a security incident, the SOC team will manage it centrally, at the SOC. This requires access to all security tools from a single location, as well as access to data from all systems and segments in real-time, to investigate it during the incident.

Sensors

IT Sensors - Cyberbit Endpoint Detection and Response (EDR)

Cyberbit EDR is an endpoint detection and response system, which detects advanced and targeted threats that bypass conventional, signature-based security systems. The EDR sensor is installed in IT endpoints and continuously records kernel-level data from the operating system kernel level. The data is delivered to the central big-data repository. Data is analysed by means of behavioral analysis and machine learning algorithms, which detect and alert upon signs of malicious activity. The analysis is then presented to the SOC analyst who can continue the investigation using EDR tools and determine the root cause of the attack.

OT and IoT Sensors - Cyberbit SCADAShield Sensors

The SCADAShield platform detects cyberattacks and continuity risks in OT networks including IT to OT attack vectors, as well as Machine to Machine (M2M) attacks. The SCADAShield Blackbox is a non-intrusive device, which monitors the entire OT network and industrial IT components such as HMI workstations, SCADA servers and

"The building's security operations are managed centrally, at a Security Operations Center (SOC). SOC managers and analysts must have 24/7 situational awareness across IT, OT and IoT segments and have access to data, dashboards and reports, which visualise security systems in a central location, and provide cross-segment information and context in the event of an IT/OT attack."

historian servers. It performs passive and non-intrusive Deep Packet Inspection (DPI) of OT network transmissions, with granular analysis down to the field level, including both Ethernet and serial communications. SCADAShield provides out-of-the-box support for the majority of ICS/SCADA protocols, and continuously adds support for new and proprietary protocols. SCADAShield also creates a real-time network map providing full visibility of the OT network, and identifying risky IT/OT touchpoints.

Architecture: Layered Approach

Cyberbit uses a layered approach when implementing a smart building project:

Layer 1: Management layer

Security operations are centralized in the SOC, which collects all security data from IT, OT and IoT systems, with a SIEM solution as the ticketing system. The management layer includes big-data repositories for IT, OT and IoT based on Cyberbit's EDR and SCADAShield products. They perform behavioral analysis and machine learning to detect threats and business continuity risks, and provide investigation and forensic tools.

Layers 2-5: Structure-Monitoring Layers

OT/IoT security is implemented in 4 layers. Each one includes an instance of the SCADAShield system, with 8 SCADAShield black-boxes providing deep packet inspection across the operational network.Each environment is designed as an isolated network with a 3rd party firewall and switch integrated by Cyberbit.

Layer 6 - Security Staff Layer

This layer monitors all security equipment including IP cameras, motion detectors, and intercom systems. It includes Cyberbit EDR sensors for IT Endpoint Detection, which are installed on all security staff workstations and IT servers.

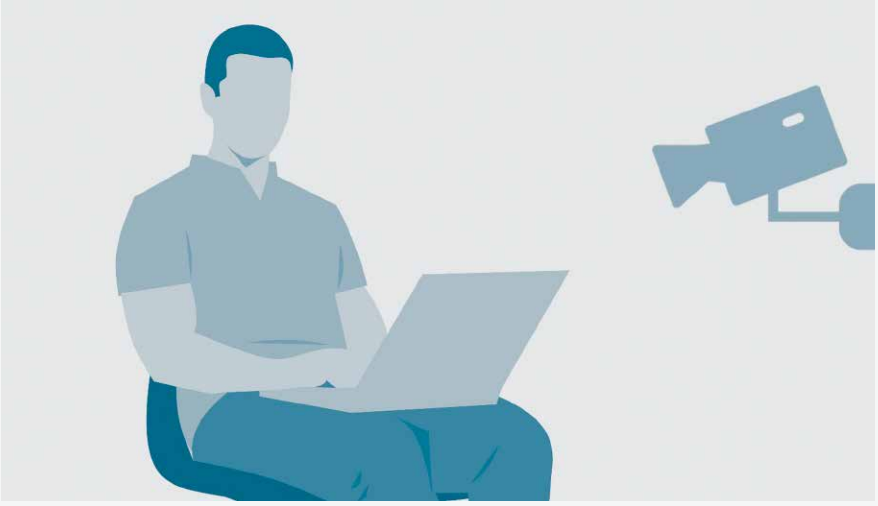
For more information, please visit: www.cyberbit.com SST

Did you Know?

There will be an estimated 200 billion connected IoT devices by 2020. The Cyber Shield Act of 2017 introduced by American Senator Edward J. Markey requires IoT vendors to follow "security-by-design" best practices in accordance with the National Institute for Standards and Technology (NIST) allowing buyers to assess the associated risks of purchasing a product.

Security and Surveillance Integrator Universal Alarms Solves Northrop Grumman's Video Surveillance Storage Issue

Northrop Grumman was searching for a purpose-built video surveillance storage solution that could handle 40-50 IP Cameras all running 3MP resolution, at full 30 Frames Per Second (FPS) and continuous recording 24/7 including low light night-time operations. Universal Alarms and Arxys made it happen. Northrop Grumman turned to experienced security and surveillance integrator Universal Alarms to solve their needs for performance, protection and price.



Challenges

Operating a top-level secure site for classified projects for the federal government that requires the highest levels of physical security and controlled access around the clock is challenging. Configuring a high performance video surveillance system to provide security for that site that pushes the boundaries of IP Camera frame rates, multi megapixel resolutions and 24/7 continuous recording is equally as challenging. Getting that ultra high performance, high availability and HD video optimised video surveillance system to come in on time and under budget is extremely challenging.

Northrop Grumman was searching for a purpose-built video surveillance storage solution that could handle 40-50 IP Cameras all running 3MP resolution, at full 30 Frames Per Second (FPS) and continuous recording 24/7 including low light nighttime operations. Northrop Grumman required high availability that eliminated most single points of failure to ensure always-on security. Complicating matters was a budget crunch that kept a tight lid on the total solution budget.

Northrop Grumman turned to experienced security and surveillance integrator Universal Alarms to solve their needs for performance, protection and price. Universal Alarms, as a long term Arxys partner and experienced security integrator knew that the combination of requirements, budget and security required tight coordination. Arxys had helped Universal Alarms solve many other clients video surveillance needs and this proved to be no exception.

Solutions

Working with Arxys experienced surveillance solutions team Universal Alarms and Northrop Grumman were able to utilize the Arxys | Shield Appliance integrated with Valerus VMS and supporting up to 150 ultra high resolution cameras.

The Arxys | Shield Appliance running Valerus VMS on purpose-built optimized hardware delivered the multi-streaming throughput performance, 24/7/365 availability and price performance required by Northrop Grumman. Not only did the Arxys appliance outperform other video surveillance products while providing scalability and advanced data protection; it delivered the lowest TCO of any comparable system.

Benefits

Universal Alarms has another extremely satisfied customer whose security and surveillance system runs continuously

> "The surveillance solutions that Arxys provides easily handle current needs while ensuring we can grow and scale with more cameras, HD resolutions and ever longer retention times. Our customers love the solutions, the simplicity and the data protection."
>
> ***- Nick Kaufman, Universal Alarms***

without a hitch. Northrop Grumman now has a rock solid security and access control solution that delivers round the clock surveillance, HD multi-streaming performance and advanced data protection. They also have plenty of room to seamlessly scale the number of cameras and applications thanks to Arxys' pay as you grow scalability. Their initial 48TB's of surveillance storage can be doubled to 96TB's seamlessly and easily to accommodate growth.

> "The Arxys video surveillance system is the best kind of system: It just works. High frame rates, maximum HD resolutions, 24/7 continuous recording at 3 Megapixels with zero downtime or hiccups. Solid and secure video surveillance that works really well."
>
> ***- Security Director, Northrop Grumman***

Arxys |Shield Appliance's redundant hot-swap power supplies, hot-swap hard drives, advanced SMART alerts and RAID 5 data protection ensured non-stop operation and accessibility to all surveillance videos. The pre-configured Vicon VMS and optimised video processing made installation and setup a breeze.

The surveillance system is effective and does what all great appliances do: it just works. The security team at Northrop Grumman never has to think about the hardware at all and can just focus on securing the facility. Arxys Surveillance Storage Servers solve surveillance problems so you can provide security and protection.

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

HD IP Delivers Clear Benefits for Tower Transit

As camera technology evolves, operators are beginning to see the benefits of integrating high definition (HD) IP cameras into their surveillance solutions. Not only is the footage they collect more detailed, IP cameras can save operators money in fines and compensation, whilst providing an unbeatable training tool.

Thinking big – Fleet Wide IP

The Tower Transit Group employs 2,930 staff and operates 1,030 buses in some of the worlds most connected and busy cities, where there is immense pressure on drivers to transport commuters safely and efficiently. London is one such city.

With 450 buses operating within the TfL London framework, Tower Transit London needed to ensure its use of surveillance technology was supporting every aspect of operations. Fulfilling that need saw Tower Transit become one of the first operators to implement forward-facing IP cameras.

Making the Switch

Tower Transit has had forward-facing analogue cameras fitted to vehicles since 2015. The cameras capture clear, quality footage from the road in front of the vehicle and record vital data for training, journey analysis, law enforcement and insurance or other claims – which can be reviewed by the CCTV analysts based at the depot.

A review of their on-board surveillance capacity highlighted a number of instances where footage retrieved from the legacy forward-facing cameras had not always been clear enough to rebuke insurance claims, e.g. partial registration plates being recorded or out-of-focus footage, so Tower Transit approached Synectics for a solution.Synectics demonstrated the superior image clarity that HD IP cameras could deliver, as well as increased functionality, such as the ability to zoom in without quality loss – essential for helping drivers and operators to see things in precise detail, including number plates and cyclist positions on the road.

Tower Transit initially trialled forward-facing IP cameras with Synectics on vehicles in 2015, before updating their specification to include them on every new vehicle that leaves the factory.

Greg Wright, Insurance Manager, Tower Transit Operations Ltd said: “Imagine watching a football match on a HD TV screen. You can see each blade of grass, facial expression of the player and the picture quality stays in focus despite movement following the ball up the pitch. Then imagine going back to viewing a football match on an LCD or SD TV screen – you just wouldn’t! Well that’s exactly how I feel about installing IP cameras on our fleet. Analogue cameras are absolutely fine. They do the job and the majority of the time the footage captured gives you the evidence that you require. However, if you’ve ever viewed an incident and wished that you could just zoom into a vehicle registration number plate, or even a passenger’s face, then you’ll appreciate the benefits that IP can offer. We certainly wouldn’t go back to analogue”.

“Analogue cameras are absolutely fine. They do the job and the majority of the time the footage captured gives you the evidence that you require. However, if you’ve ever viewed an incident and wished that you could just zoom into a vehicle registration number plate, or even a passenger’s face, then you’ll appreciate the benefits that IP can offer. We certainly wouldn’t go back to analogue”.

- Greg Wright, Insurance Manager, Tower Transit Operations Ltd

A Truly Integrated Solution

Installed to the dashboard, these forward-facing road IP cameras are part of their overall on-vehicle surveillance solution, including analogue interior and exterior cameras, and driver’s cab monitors and, because the migration to IP can be an evolutionary process, Tower Transit is able to strategically target when and where IP cameras are implemented. During the transition, Synectics offers expert guidance and provides flexible options – an approach suitable for operators of any size, with any budget. New vehicles (and any requiring upgrade), are also fitted with Synectics’ hybrid T1600 digital video recorder (DVR) with Synectics’ integrated management platform – Synergy 3 Transport – being utilised to monitor and review the T1600 footage. Synergy 3 Transport gives Tower Transit a new level of flexibility and technical capability for managing on-vehicle security and surveillance, whilst effectively and efficiently managing their fleet.

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

VA Healthcare Facility Turns to PSIM for an Integrated Security Solution that Meets Compliance Regulations

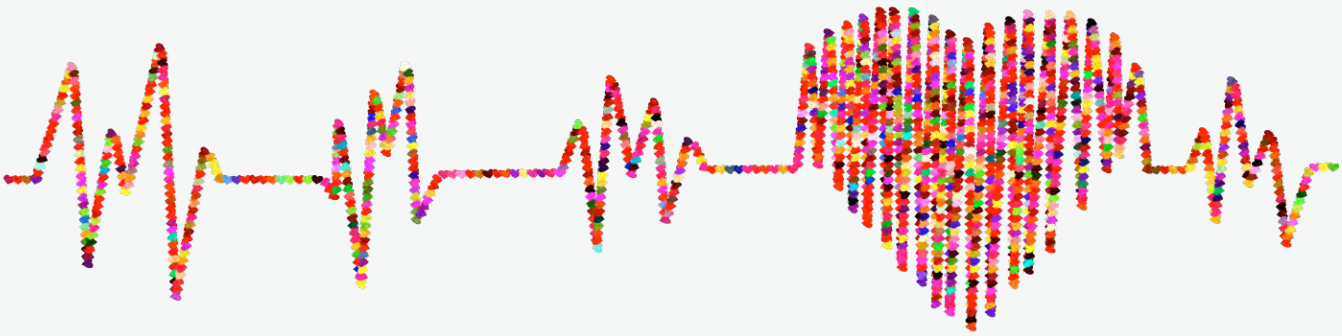
Challenge

A U.S. Veterans Administration healthcare facility’s need to comply with HSPD-12 requirements led to concerns over its lack of centralised, integrated control. It was managing two expensive legacy surveillance systems (analog CCTV and IP-based), had an outdated access control system, and wanted to reduce costs associated with long-term infrastructure (bandwidth, power and space) and security operator training. The facility also wanted to be able to generate security system reports more efficiently.

The customer was weighing two alternatives. The first option was to completely replace its existing security system, which would standardise its security onto a single VMS platform and accelerate a move to a total IP-based video security system. The other option was to implement a command and control functionality across all of its legacy analog and new IP-based systems.

Solution

After reviewing the costs associated with replacing the systems, training



and overall transition, the customer decided on the second option, deploying a Physical Security Information Management (PSIM) system. This security solution allowed the customer to integrate all of its systems under one, user-friendly Graphical User Interface (GUI) and to migrate to new systems without scrapping its existing investments. The customer also chose this solution for its reduced report generation time (from days to minutes), improved situational awareness and its ability to integrate with new systems in the future.

Implementation

The PSIM solution was implemented to manage hundreds of cameras and readers and nearly 1,000 alarm points. All sensors and other data were integrated onto a video wall display that is updated in real time. Two full-time security operators manage the system across three shifts. The healthcare facility's response procedures are now automatically tied to alerts by type, and many functions are automatic or require only single-click operation. Imbedded alert reporting and automatic report generation help save operator time. The entire project was completed under budget.

Results

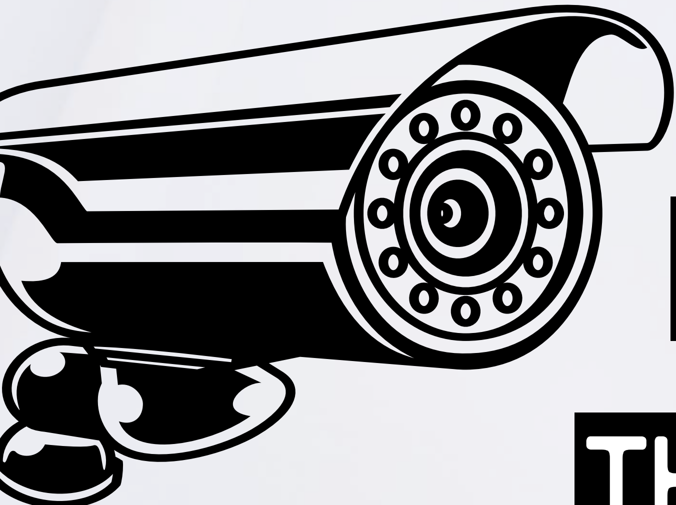
Implementing PSIM has provided significant cost savings in manpower and equipment in comparison to total system replacement. Long-term cost savings will result from reduced training, increased employee productivity, and improved operator efficiency.The PSIM solution also offers the customer integration support for its existing systems and published, well-documented SDK for additional integration.

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

"The PSIM solution was implemented to manage hundreds of cameras and readers and nearly 1,000 alarm points. All sensors and other data were integrated onto a video wall display that is updated in real time. Two full-time security operators manage the system across three shifts. The healthcare facility's response procedures are now automatically tied to alerts by type, and many functions are automatic or require only single-click operation. Imbedded alert reporting and automatic report generation help save operator time. The entire project was completed under budget."

Did you Know?

According to the Philips Lighting and SmartCitiesWorld report, the top 3 SMART cities in the world are Singapore, London and Barcelona. Singapore for its futuristic infrastructure design and utilisation of urban spaces, London for its focus on communities and technology implementation and Barcelona for its governmental initiatives redefining smart cities.



SURVEILLANCE STEPS UP THANKS TO TECH MAKEOVER

2018 CCTV Surveillance Trends to Watch Out For

As technology continues to advance rapidly, the demand for dynamic CCTV security systems is becoming increasingly prominent. Regardless of whether it is Facility security, traffic management, or in support of the wider Internet of Things trend, CCTV solutions are infiltrating the surveillance market. According to industry research, over 98 million network surveillance cameras were shipped in 2017, globally.

Rise in Data Being Used to Supplement Video Analytics

As business security systems become more complex, it's going to become imperative for organizations to become more adept at leveraging data to identify patterns and trends in their organisation. Surveillance video data will become increasingly more significant, not only for keeping people and property safe but also to help the business yield better financial returns by tracking patterns and trends. Video analytics applications that can be highly granular and sophisticated will become adopted more and more to help businesses make better decisions.

Intelligence Inbuilt Surveillance Cameras

It's been predicted that 2017 will yield an accelerated adoption of cameras with wider panoramas, higher resolutions, and more accurate sensors. Camera installations will transition from standalone analog and SD cameras as demand for cameras with more embedded surveillance capabilities compression, streaming, storage, and analytics , increases. It is worth noting that, as the influx of data continues, storage will become strained and a comprehensive, multi-tier storage strategy will be vital.

CCTV Systems Become Crucial for Healthcare Organisations

As the need for stricter security in hospital and healthcare organisations continues to be a priority in the industry, having comprehensive CCTV security systems will be crucial to keeping the facilities safe and secure. Currently, 80 percent of hospitals need to upgrade their access control systems and CCTV solution to meet International Association for Healthcare Security and Safety (IAHSS) guidelines. As the needs of hospitals and healthcare organisations continue to change and adapt, a modern CCTV security system will be imperative to improve overall facility safety and security while also increasing operational efficiency.

> *"Currently, 80 percent of hospitals need to upgrade their access control systems and CCTV solution to meet International Association for Healthcare Security and Safety (IAHSS) guidelines. As the needs of hospitals and healthcare organisations continue to change and adapt, a modern CCTV security system will be imperative to improve overall facility safety and security while also increasing operational efficiency."*

Biometric Applications to Become More Prevalent

Biometric applications are predicted to hit a boom in the coming years. From healthcare organisations increasingly adding facial recognition to their security suite to using fingerprints to help keep track of people and prevent congestion on transportation services, biometric applications are becoming more widely used among many industries. More and more, biometric applications are becoming a critical component in preventing major data breaches.

Internet of Things (IoT) Boosts Potential for Integration

As the trend of Internet of Things – when interconnected everyday devices are able to send and receive data via the internet – continues to become more of a norm, video data with input from smart devices is becoming more robust and secure. IoT systems can be integrated with and supported by video to provide information for facility, operational, or business needs. Video analytics like heat mapping and person counting can also help business gather more business intelligence and strengthen security.

The Move Towards Cord-Free Continues

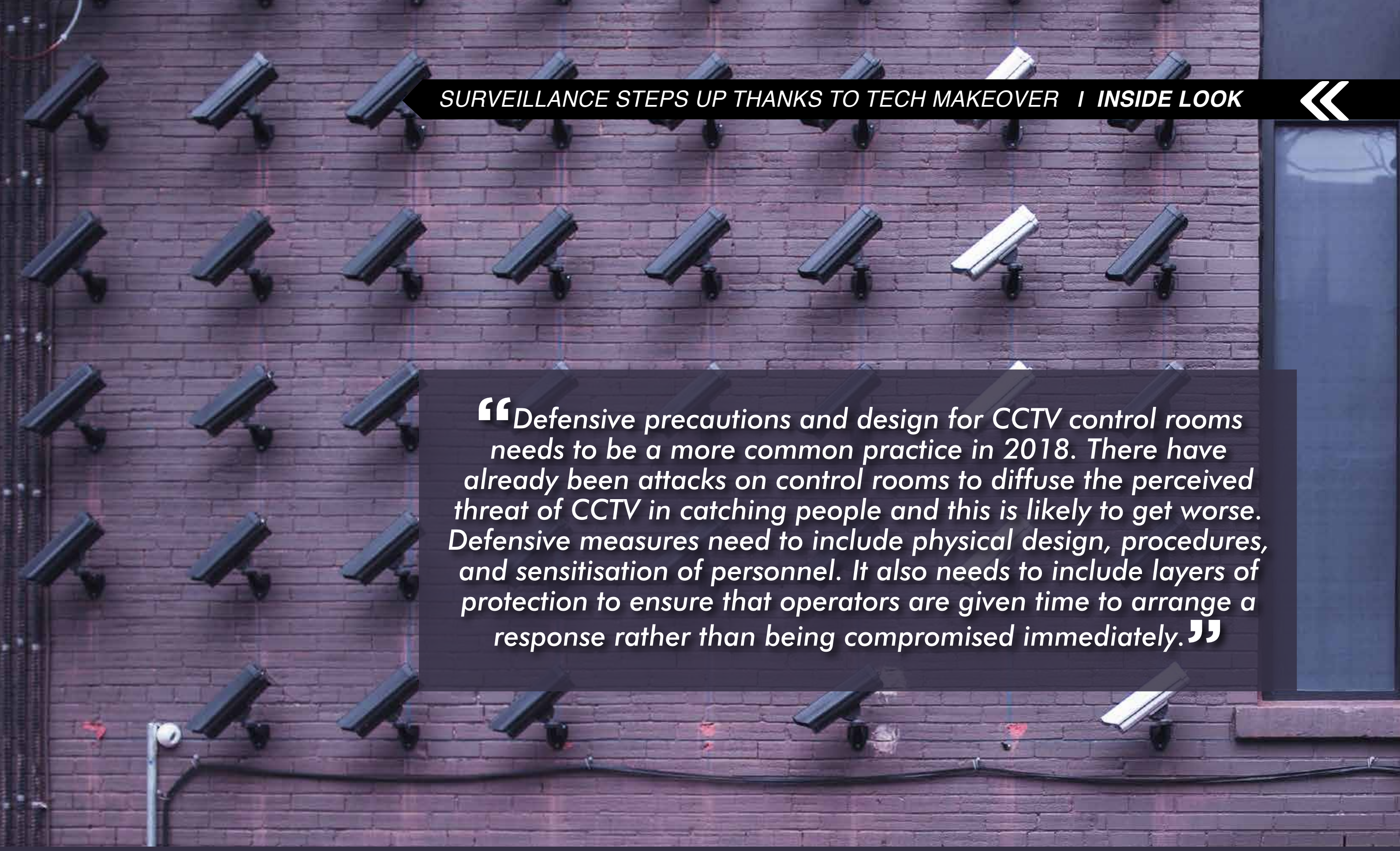
Wireless technology has transformed our day-to-day lives in many ways and its influence on the CCTV system industry is no different. Multi-camera video surveillance systems are now able to be managed entirely via mobile devices. This helps with ease of use of the technology while also reducing overall system and maintenance costs.Many businesses and organisations can benefit greatly from having a dynamic security and monitoring system in place.

Integration and Analytics

2018 will also see some serious decision-making on whether to go for an integrated control room incorporating CCTV, or to have a specialised function. Too many companies have been diluting the CCTV content to the extent that they have no viable surveillance function which could be expected to pick up things independently. The ongoing inclusion of a whole range of functions in the control room has meant that operators have less and less time to check what is happening on their CCTV monitors. The pressure on performance is going to force decisions on whether to have multipurpose control rooms where detection becomes a secondary consideration, or to separate out surveillance as a real function.

Video analytics will continue trying to find a home broader than simple recognition function. They are simply not delivering on their promises of previous years. However, two main trends will emerge in respect of analytics. The first is to have them contribute to human focused problem solving. For example, in the UK, face extraction software and recognition of body build and clothing characteristics are being used to assist Super Recognisers identify and trace suspects.

The other real benefit of video analytical capabilities is for integration into bigger systems which can use pattern analysis findings in conjunction with a whole range of other criteria and data sources including access control and crime trends to create better intelligence systems. This includes going for



"Defensive precautions and design for CCTV control rooms needs to be a more common practice in 2018. There have already been attacks on control rooms to diffuse the perceived threat of CCTV in catching people and this is likely to get worse. Defensive measures need to include physical design, procedures, and sensitisation of personnel. It also needs to include layers of protection to ensure that operators are given time to arrange a response rather than being compromised immediately."

integration with other sources in surrounding areas, where broader communities can pool data to discover suspects and track them. The use of intelligent systems along with supplementing operations with skilled analysis and extended database usage has some of the best potential to fight crime in the industry.

Cybersecurity is Very Necessary

CCTV systems are going to get hacked electronically and we probably won't even get to know about it. The volume of systems and levels of protection mean there are just too many opportunities for those wanting to exploit vulnerabilities. In a similar vein, we can expect more jamming of CCTV systems to occur as part of criminal strategies.

While the CCTV acronym refers to the physical linking of cables and equipment into a 'circuit', we already have jamming of your car alarm and of vehicles in major logistics companies. Expect this kind of approach to spread to CCTV installations relying on wireless, cell and other types of transmissions. Companies need to start having a look at having 'Plan Bs' in place for such events.

Defensive precautions and design for CCTV control rooms needs to be a more common practice in 2018. There have already been attacks on control rooms to diffuse the perceived threat of CCTV in catching people and this is likely to get worse. Defensive measures need to include physical design, procedures, and sensitisation of personnel. It also needs to include layers of protection to ensure that operators are given time to arrange a response rather than being compromised immediately. Crowd surveillance strategies are going to become even more important this year especially in public areas where community issues are often being fought out on the streets.

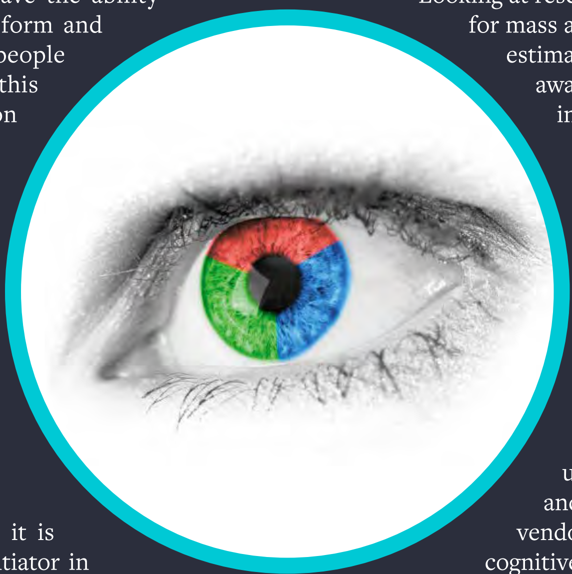
Camera ranges are going to expand including thermals, mobile cameras, drones, 180- or 360-degree cameras. Many of these call for an enhanced understanding of what is being looked at and how to look at it. This means that their use needs to be made part of a security strategy and people using them need to be trained and sensitised in how to get the benefits of such tools. It is no use just having lots more cameras or different types. How these play a part in a defensive CCTV strategy is even more important to define their roles and the use to which information is going to be put. Even more than before, operators are going to have to know what they are looking for.

Security managers are going to have to justify practices in view of incoming legislation and public issues. Companies are going to be burnt because they didn't think of the implications of use, or the possible challenges that may arise as to how they use CCTV. Questions around access to data are going to cause a lot of managers headaches.

There may be more of a professional approach to staffing in CCTV operations. This is an issue that has been around for years with little thought about the quality of selection, training or placement of people in CCTV positions. The best companies using CCTV all address these issues in order to be successful and clearly stand out in the industry. However, for many, the quality of people is secondary to a cheap cost and placement of people on seats. SST

TOP TECH TRENDS FOR THE SECURITY INDUSTRY IN 2018 AND BEYOND

It started with the Internet of Things that is also fondly known as the Internet of Everything. This opened up the doorway to Artificial Intelligence and Machine Learning. Industries and various sectors such as law enforcement and even border security are welcoming a new wave of technologies that have the ability to not only enhance but also transform and completely revolutionise the way people and properties and protected in this connected age. While digitalisation of the security industry definitely has its benefits, the risks are also eminent as more and more devices including barriers and access control are connected to the cloud. As we proceed further into 2018, it is clear that this disruptive yet diverse technology is here to stay. Trends taking off this year include:



Artificial Intelligence (AI)

AI has matured to the point where it is being used as a competitive differentiator in several industries, particularly in the smartphone, automotive and medical markets. Also, optimisation for on-device versus cloud-based solutions is becoming an area of focus. Cloud AI has more computing power to analyse data as while utilising deep learning algorithms, but there are potential issues around privacy, latency and stability. On-device AI, meanwhile, can help offset those dangers to some degree. For instance, smartphone users who deploy the built-in AI of their phones are able to store data locally and thus safeguard their privacy.

Looking at research from prominent analysts, plans for mass adoption are very promising. Gartner estimates that AI is about two-five years away from mainstream adoption, for instance, and 75% of executives polled by the Economist Intelligence Unit think AI is so important they plan to implement in their business within the next three years.

Video analytics is another area where AI techniques, such as deep learning algorithms, are broadly applied. In the security industry a number of vendors provide “black box” video analytics that can be used for non-scan detection at PoS and object recognition, but the big tech vendors are taking this further by offering cognitive services in the Cloud.

Internet of Things (IoT)

The global installed base of IoT devices will rise to 73 billion in 2025, IHS Markit forecasts show. Accelerating IoT growth in 2018 and movement through a four-stage IoT evolution

> *"Gartner estimates that AI is about two-five years away from mainstream adoption, for instance, and 75% of executives polled by the Economist Intelligence Unit think AI is so important they plan to implement in their business within the next three years."*

"Connect, Collect, Compute and Create" will be the confluence of enhanced connectivity options with edge computing and cloud analytics.

Enhancements in IoT connectivity, such as low-power wireless access (LPWA) will drive growth. Moreover, technologies adjacent to the IoT will become increasingly sophisticated. Machine video and ubiquitous video will empower new types of visual analytics. AI, the cloud and virtualisation will help develop critical insights sourced from data at the so-called "edge" of computing networks. Applying AI techniques to data will drive monetisation in the form of cost savings, greater efficiencies and a transition from product- to service-centric business models.

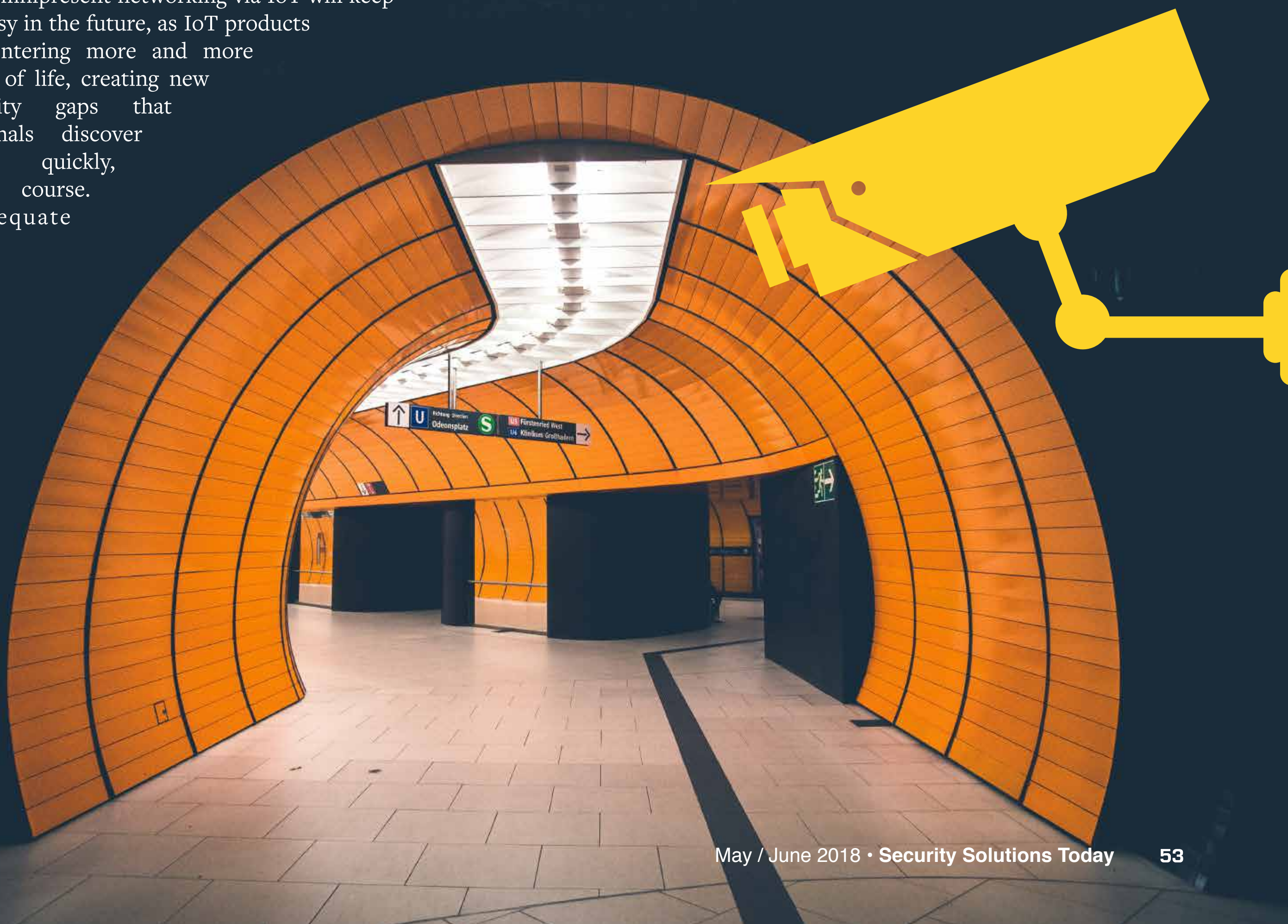
Security companies have grasped this opportunity by developing biometric and facial recognition cameras, digital locks, remote sensors alarm, etc. But with security system being controlled remotely, cyber security becomes a critical risk. The security industry is shifting its focus from the physical defence and hardware to the software and encryption of communication.

The omnipresent networking via IoT will keep us busy in the future, as IoT products are entering more and more areas of life, creating new security gaps that criminals discover very quickly, of course. Inadequate security solutions and data protection problems make it easy for them, but there have also already been discovered huge botnets that consist of IoT-like devices that implemented DDoS attacks to such a frightening extent.

Cloud and Virtualisation

Cloud services will pave the way for technologically immature companies to utilise machine learning (ML) and AI, radically transforming their usage and understanding of data.

However, a weakness in physical security can be just as dangerous as any vulnerability in cyberspace. An improperly protected or suboptimally located data center can put important information and operations at severe risk of disruption. In addition to thieves and natural disasters, enterprises face possible danger from unauthorised employees having access to loosely secured server rooms. Accordingly, it is imperative that organisations approach cloud security holistically and devote adequate attention to both protecting data and securing the physical locations in which it resides.



"Video analytics software for security cameras is available in several forms: installed on your camera, on your NVR, or as 3rd party software you buy. Each version will do the same thing, however - monitor your videos to search for and alert you to activity. Each video analytics solution will work a bit differently depending on the manufacturer and application."

Connectivity

As the first 5G commercial deployments emerge, the story will focus on connectivity. The path to full 5G adoption and deployment is complicated, with new opportunities and challenges alike in store for mobile network operators, infrastructure providers, device manufacturers and end users. 5G represents a dramatic expansion of traditional cellular technology use cases beyond mobile voice and broadband, to include a multitude of IoT and mission-critical applications.

Communication security is a fundamental requirement for 5G and, specially, for IoT and MTC, given the wide range of commercial, industrial, and military applications. Current security techniques are mainly based on cryptographic methods employed at the upper layers of communication protocols, assuming that the eavesdropper has limited computational power. This assumption, however, is becoming an issue nowadays since computational power is ever growing.

Ubiquitous Video

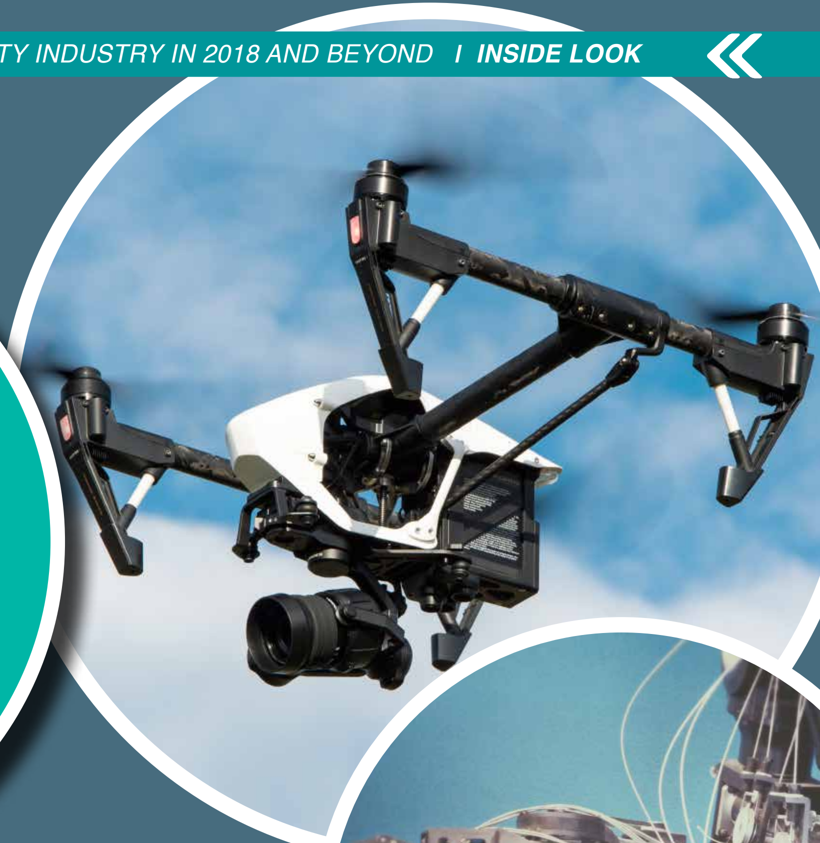
The growing use of screens and cameras across multiple consumerand enterprise-device categories, along with increasingly advanced broadcast, fixed and mobile data networks, is powering an explosion in video consumption, creation, distribution and data traffic. More importantly, video content is increasingly expanding beyond entertainment into industrial applications for medical, education, security and remote controls, as well as digital signage.

More screens translates to more footage and fottage itself is evolving accordingly. Video analytics software was created to help review the growing hours of surveillance video that a security guard or system manager may never have time to watch - your video surveillance system is only as useful as the incidents you can actually capture and watch, and video analytics will help you find them.

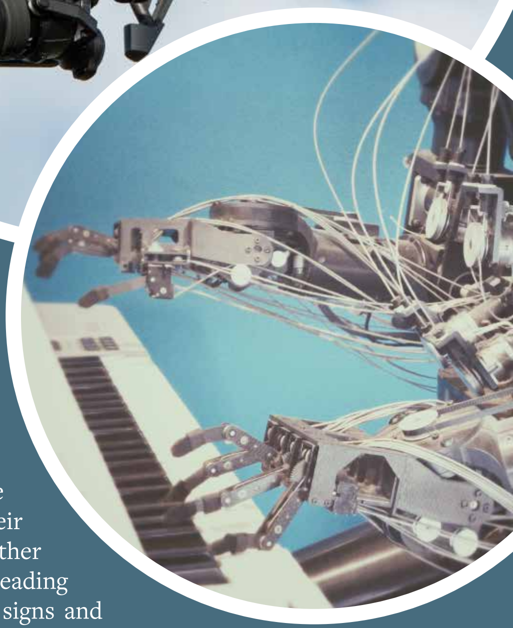
Using video analytics makes your surveillance system more efficient, reduces the workload on security and management staff and helps you capture the full value of security video by making your IP camera system more intelligent in its work.

Video analytics software for security cameras is available in several forms: installed on your camera, on your NVR, or as 3rd party software you buy. Each version will do the same thing, however - monitor your videos to search for and alert you to activity. Each video analytics solution will work a bit differently depending on the manufacturer and application. They all work in the same basic way, however - when setting up the software you set up parameters to the activity the software is looking for, set up the alert notification system, and when the software detects something that meets its search criteria it alerts you.

The old idea of a video surveillance system is of a security guard sitting in a booth watching the security camera feed live, hoping to catch suspicious activity. This model relies on having a live person watching and reviewing all your video, however, which is not practical or efficient. Different security guards may have differing levels of focus or different ideas of suspicious activity.Video management software changes this system by using software to monitor your video feed around the clock, alerting you to activity so you only need to watch the cameras when something happens. This will help you best utilise your surveillance system, saving you time and effort.



"The global market for robots and drones will grow to $3.9 billion in 2018. The deeper underpinnings of the story, however, lie in the disruptive potential of robots and drones to transform long-standing business models in manufacturing and industry, impacting critical areas such as logistics, material picking and handling, navigational autonomy and delivery."



Computer Vision

The increasing importance of computer vision is directly tied to the mega-trend of digitisation that has been playing out in the industrial, enterprise and consumer segments. The proliferation of image sensors, as well as improvements in image processing and analysis, are enabling a broad range of applications and use cases including industrial robots, drone applications, intelligent transportation systems, high-quality surveillance, and medical and automotive.

The rise of digital business creates major challenges for the modern security organisation. Operational technology and the Internet of Things (IoT) massively expand the scope of security strategy and operations and expose gaps in the skills of the security organisation. Simultaneously, we must still maintain our foundational IT capabilities and services.

Robots and Drones

The global market for robots and drones will grow to $3.9 billion in 2018. The deeper underpinnings of the story, however, lie in the disruptive potential of robots and drones to transform long-standing business models in manufacturing and industry, impacting critical areas such as logistics, material picking and handling, navigational autonomy and delivery.

Low-cost drones and robotic systems combined with rapid advances in machine learning, are making it possible to automate whole sectors of low-skill work. While there is plenty of worry about the automation of jobs in manufacturing and offices, routine security and safety inspections may be one of the first big areas to be undermined by advances in AI.

Robots are increasingly being used for security and surveillance applications, as well as the traditional Bomb Disposal and search & rescue roles. Now personal robots are available in the $40,000 – $300,000 range and are used as nighttime watch keepers by their owners, as well as other tasks like recipes, reading news, monitoring vital signs and alerting help if someone falls. There is practically no limit to what a robot can be programmed to do these days. With multiple cameras, laser sensors and sonar, these wi-fi enabled portable scanning machines can tell you anything you want to know about their surroundings, including if a burglar has broken into the office. They also make really great tele-conference terminals.

Blockchain

Blockchain enables decentralised transactions and is the underlying technology for digital currency such as bitcoin and ether. Blockchain-based services beyond financial services are already being developed and deployed and will continue to ramp in 2018. These include: the use of blockchain to improve advertising measurement and combat ad fraud; blockchain-based systems for distributing music royalty payments; and solutions to better track and manage electronics supply chains. Clive Longbottom, an analyst at Quocirca, is positive about its use to secure IoT."When applied to the IoT, Blockchain can provide the much-needed verification of data source, preventing the man-in-the-middle (MiTM) attacks that threaten to become commonplace," he said. By doing away with a central authority in internet of things (IoT) networks, blockchain technology can reduce the risk of IoT devices being compromised by a single point of security failure. SST

Modern IP surveillance cameras are now offering *a wealth of additional functionality, such as deep learning analytics, facial recognition, as well as multi-sensor and multi-directional motion detection, which can be integrated into solutions across building and transport solutions, city infrastructure, defence, industrial, defence and commercial settings.*

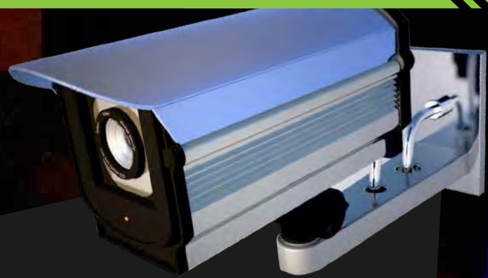
IC Realtime is Google for CCTV. *It is an app and web platform named Ella that uses AI to analyse what is happening in video feeds and make it instantly searchable. Ella can recognise hundreds of thousands of natural language queries, letting users search footage to find clips showing specific animals, people wearing clothes of a certain color, or even individual car makes and models.*

SeeQuestor's CCTV system can recognise someone, *track him or her through a crowd with footage from one camera, then pick that person out of the same crowd with another even if it temporarily loses sight of him or her. In the near future, the company's plan is to give the system a more detailed suite of characteristics to track people with - hair length, glasses, clothing colour - a bit like digital game of Guess Who, but the character on the last unflipped tile gets arrested.*

THE FUTURE OF CCTV

BIG BROTHER BOT AND BIG DATA ARE WATCHING

Manufacturers are looking to equip their CCTV systems *with such capabilities as Facial recognition software, enabling home security to automatically recognise a person from their image on the camera and allow/deny entry to the property as a result and integrated alarm sensors to be placed on windows around the home for centralising all of the security in one central command unit. Other features such as tracking car registration plates and monitoring traffic patterns to give up-to-the-minute information on potential transgressors and best routes for navigation, the ability to control the security apps via text or voice commands and to recognise unconsciousness in a person and summon emergency services as a result, are also in the works.*



High-performance cameras are now smaller, *lighter and more easily embedded into drones. As a result, airborne surveillance cameras will become more commonplace within a short period of time, supplementing and, in some cases, supplanting the more familiar fixed-position CCTV cameras we see today. An unmanned aerial vehicle (UAV) will be capable of tracking moving subjects thanks to its laser sensors. Upon technology improvement drones will likely patrol at-risk areas 24 hours a day, acting as a deterrent against break-ins. 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.*

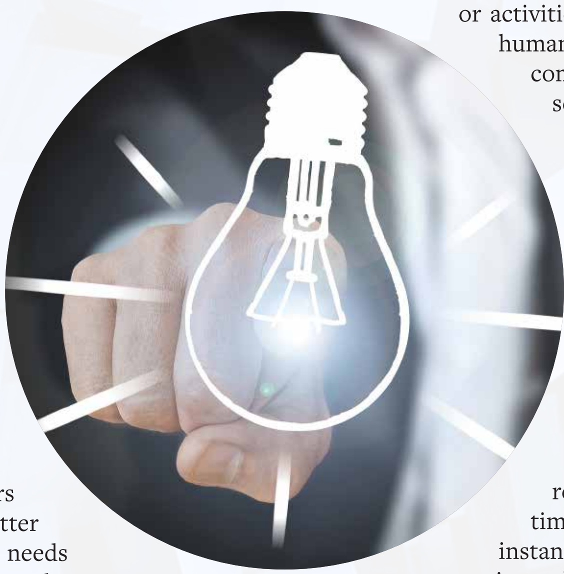
Emotion reading technology could soon *be used by police after a Russian firm created a tool that can identify people in a crowd and tell if they are angry, stressed or nervous. The software, created by NTechLab, can monitor citizens for suspicious behaviour by tracking identity, age, gender and current emotional state. It could be used to pre-emptively stop criminals and potential terrorists. The identification app claims to have reconnected long-lost friends and family members, as well as helped police solve two cold cases and identify criminals.*

INTERVIEW WITH

MS. TAN KHAI HUA, HEAD OF MARKETING AND COMMUNICATIONS AT SOVERUS CONSULTANCY & SERVICES PTE LTD

Could you share with us on the recent developments in CCTV technology and how this new technology such as IP Cameras, facial recognition software and even data analytics assist in enhancing security?

IP cameras have been around for a while and have proven to allow better connectivity as well as better data processing that are required for today's CCTV applications. Recently, facial recognition technology has also been added to such cameras to provide added capabilities to capture and identify the person. Together with data analytics, such technology also helps to cut down the processes and time needed to manually match faces against existing database, making it an essential part of security, especially in today's high level of security alertness.



In addition, significant improvements in facial recognition technology and CCTVs, as well as the reduction of costs are making this capability available to a wider range of industries and applications beyond security. Besides deployment at high security environments such as airports and immigration check points, where fast and precise recognition of known criminals is critical, such technology were also introduced in marketing and business intelligence in sectors like retail and hospitality to better understand consumers' and visitors' needs and profiles. This eventually facilitates better retail outcome and service quality.

These days, even providers/integrators of physical security solutions are being forced to confront the issue of cyber security due to the Internet of Things (IoT) and the risk of CCTV being hacked. Please share with us your experience in dealing with this issue.

We have to take cognizance of the importance of data that is captured under the different physical security point systems. As we deploy these solutions, we also put in place a series of cyber security protection applications to ensure that databases and end-points are suitably protected.

What is your opinion on security robots and artificial intelligence being used to substitute or complement human security guards? Do you think they are more of an asset, a liability or both to security and safety?

The deployment of robots and AI must be judicious and depends on the place and purpose. Both are useful in situations where human traffic or interaction is minimal, such as warehouses or the perimeter of huge industrial spaces. Their main function would be to deter unauthorised entry or activities. However, in areas where there is human traffic or interaction, such as at a commercial building or shopping mall, security guards are still preferred.

Based on your experience working with law enforcement and homeland security, how do you feel that technological advancements in CCTV and surveillance can help fight terrorism or crime?

Technological advancements in CCTV and surveillance can greatly reduce the time needed for both real-time and post incident investigation. For instant, faces of suspects can be processed against a database of known persons of interest.

How is your company utilising the latest in CCTV technology to assist in enhancing security in the various sectors that you cater to such as homeland security and institutional protection?

Our Secura Integrated Command Centre is able to monitor multiple sites simultaneously round-the-clock using smart IP cameras with advanced video analytics equipped with tripwire/area detection capabilities. This provides excellent

"In the next decade, the deployment of facial recognition technology will increase exponentially as privacy considerations will be less of a concern given both the advancement in data protection technologies as well as the acceptance by the general public. It will become a norm in our daily life."

security outcome and reduce the reliance on human guards.

From a consultant's point of view, could you share with us your outlook or predictions on surveillance / CCTV usage in the next 10 years? Do you see it becoming more widely used due to the new technologies and possibly breaking into new sectors?

We expect significant improvements in facial recognition technology especially with better AIs and neural algorithms from researchers. As cost continues to drop, its adoption will also become more common in the next few years, especially in the areas of marketing and business intelligence. Buyers will be spoilt for choices and may face challenges in the identifying the most appropriate solution.

In the next decade, the deployment of facial recognition technology will increase exponentially as privacy considerations will be less of a concern given both the advancement in data protection technologies as well as the acceptance by the general public. It will become a norm in our daily life.

Another application could be in hospitality where the facial recognition software could be used to automatically display specific messages or promotions to VIP guests. For example, a VIP guest could be greeted with a personalised welcome message while hotel personnel could be alerted once he or she steps into the hotel premises.

The above are only a few examples of the new CCTV and facial recognition technology, which can be used not only to protect lives but to improve service levels and user experience in many other situations. SST

COMPANY PROFILE

Secura Group Limited is a leading provider of an integrated suite of security products, services and solutions. The Group was formed through a merger of Secura Singapore Pte Ltd and its subsidiaries and Soverus Group Pte Ltd and its subsidiaries.

The Secura group of companies has been providing security printing services of value documents with anti-counterfeit features since 1976, and owns one of the largest cheque printing businesses in Singapore. With operations in Singapore, Bangladesh and Taiwan, the Group's range of value documents include bank cheques and passbook, cash vouchers, educational certificates, marriage certificates and machine-readable betting slips, amongst others.

The Soverus group of companies provides security services including security guarding, security systems integration, cybersecurity, homeland security and other security products and services. As a premium security agency in Singapore, the group provides unarmed manned security guarding services, as well as operate a state-of-the-art 24-hour command centre with remote CCTV surveillance and video analytics for round-the-clock monitoring of premises.

The Group moved into the skills training arena in 2017, when it incorporated a new business entity which was certified as a Public Approved Training Organisation to offer training modules for security and service tracks.

Secura Group also holds 20% interest in Custodio Technologies Pte Ltd, a subsidiary of Israel Aerospace Industries Ltd. The main business of Custodio Technologies is in research and development of new cyber security solutions and capabilities with a focus on cyber early warning technology.

The Group has a well-diversified clientele comprising more than 900 customers in various industries, including multinational corporations, financial institutions and government agencies.

On 28 January 2016, the Group listed on the Catalist Board of the SGX-ST.

There is a new term in the world of video analytics known as the Internet of Recognition (IoR), *meaning computer image processing can recognise, through a single frame to many frames of video, capture and analyse any object or thing and intelligently analyse what it is and what it is doing. For example, is the object a skateboard, bike, car or truck? Is it a person or a crowd of people? Are they walking, running, climbing, sitting and so on. IoR will really start to bring everything together in the future and, as technology and computer processing evolves, there will be some exciting benefits.*

Moving beyond security and safety purposes, *the use of retail analytics such as heat mapping, people counting and dwell times are assisting retailers with demographic information and usable business data that has never been accessed before using camera technology. Marketing departments are benefiting from this information, allowing them to better understand trends and allowing them to significantly improve business processes.*

SMART CCTV, INTELLIGENT SURVEILLANCE

THE DAWN OF VIDEO ANALYTICS

Companies have provided analytics capable of biometric detection of faces *with up to 99 percent accuracy and many of these software solutions have direct integration into some of the major video management system (VMS) platforms. This allows authorities to be alerted with video verification in real-time with push-notifications when a suspect is detected and there is also the ability to tap into the internet and social media platforms to link people together with a who-knows-who engine, providing critical data to authorities.*

Video captured via CCTV can essentially turn each image *into measurable and sometimes critical data for a customer. The surface has only just been scratched with regard to what information and data can be gathered by the use of video-based analysis and it is expected that in the near future, multiple systems will be able to communicate and make decisions between devices.*

When the software based video analytic solutions *are combined with standalone surveillance systems, then these measures can host a whole new range of physical security use cases. Some of these are; advanced object tracking, loitering detection, perimeter defense, intrusion detection, human traffic flow, trip wire counting, crowd density management, people counting, face indexing and audience profiling. These solutions will not only minimise the need for physical security teams but will also empower security personnel with actionable intelligence.*

Machine learning has worked to train deep learning-based systems *to recognise objects. In security and video analytics applications, the training can include behavioural traits, identification of individuals, unexpected or unusual activity, etc. This is important because it allows video analytics to be deployed with much less incident-specific configuration. Instead systems can present end-users with a range of events and incidents. The user can then decide which of these are important and which are innocuous and therefore of little interest. This will then ensure that the system only identifies events of interest.*

Real-time usage with analytics is also on the rise as public transport systems *seek to react to security events as and when they happen. With operators faced with hundreds of live feeds, alerts can assist in managing the large amount of data, helping with monitoring and prioritisation. With incidents reported in real-time, there will be more opportunity for live feeds to be shared with third parties than is reported today.*

The adoption of key technologies like Artificial Intelligence, *Edge analytics, Predictive and Reactive analytics, Machine learning algorithms, and wireless features like RFID has significantly increased the demand for video analytics in different industries like retail, city surveillance, law enforcement and fleet transportation. Uses include People management comprising of crowd detection, queue management, people counting, people scattering, people tracking as well as Vehicle management that is, Vehicle classification, traffic monitoring, license plate recognition, road data gathering. Other uses include Behavior monitoring as in Motion detection, vandalism detection, face detection, privacy masking, suspicious activity detection and Device protection for protection against camera tampering, perimeter protection, intrusion detection, theft and threat detection.*

ADOPTING A HOLISTIC APPROACH TO CYBER SECURITY

By Mark Fuentes, Senior CyberOps Consultant

Cyber security is making its way to the forefront of every enterprise's agenda. Even for organisations where cyber security is not a priority, cyber security is becoming an area of deep concern in boardrooms. As we delve deeper into the 21st century, enterprises that have been operating successfully for years and even decades with very little thought to digitisation, let alone cyber security, are scrambling to address the challenges of a cyber space full of threats.

This danger is compounded by media reports of new high-profile cyber attacks almost every other week. According to industry reports, cyber attacks are becoming more frequent and have increased in scope.

So how do businesses react to this new challenge? They throw money at the problem.

In a 2017 report by Gartner, the firm forecasts that global spending on enterprise security will reach US$96.3 billion in 2018, an increase of 8% from 2017. In the mad dash to beef up enterprise security and protect their assets from cyber threats, many enterprises fall into some bad spending habits.

Fear of Loss

In the face of an immediate threat, the natural reaction is to strengthen defenses with all haste. This is exactly the approach that businesses are taking, and understandably so as they are most concerned with avoiding loss. Much of cyber security spending is framed within the scope of how much money the business would lose in the event of a potential cyber security attack. One of the most commonly-used practices for selling cyber security solutions is to make the fear real for the decision-maker. This fear-based approach helps sell solutions but leads to poor spending practices such as supplementing existing business systems with cyber security requirements, investing in focused, specialised solutions and spending budgets in a reactive, short sighted manner.

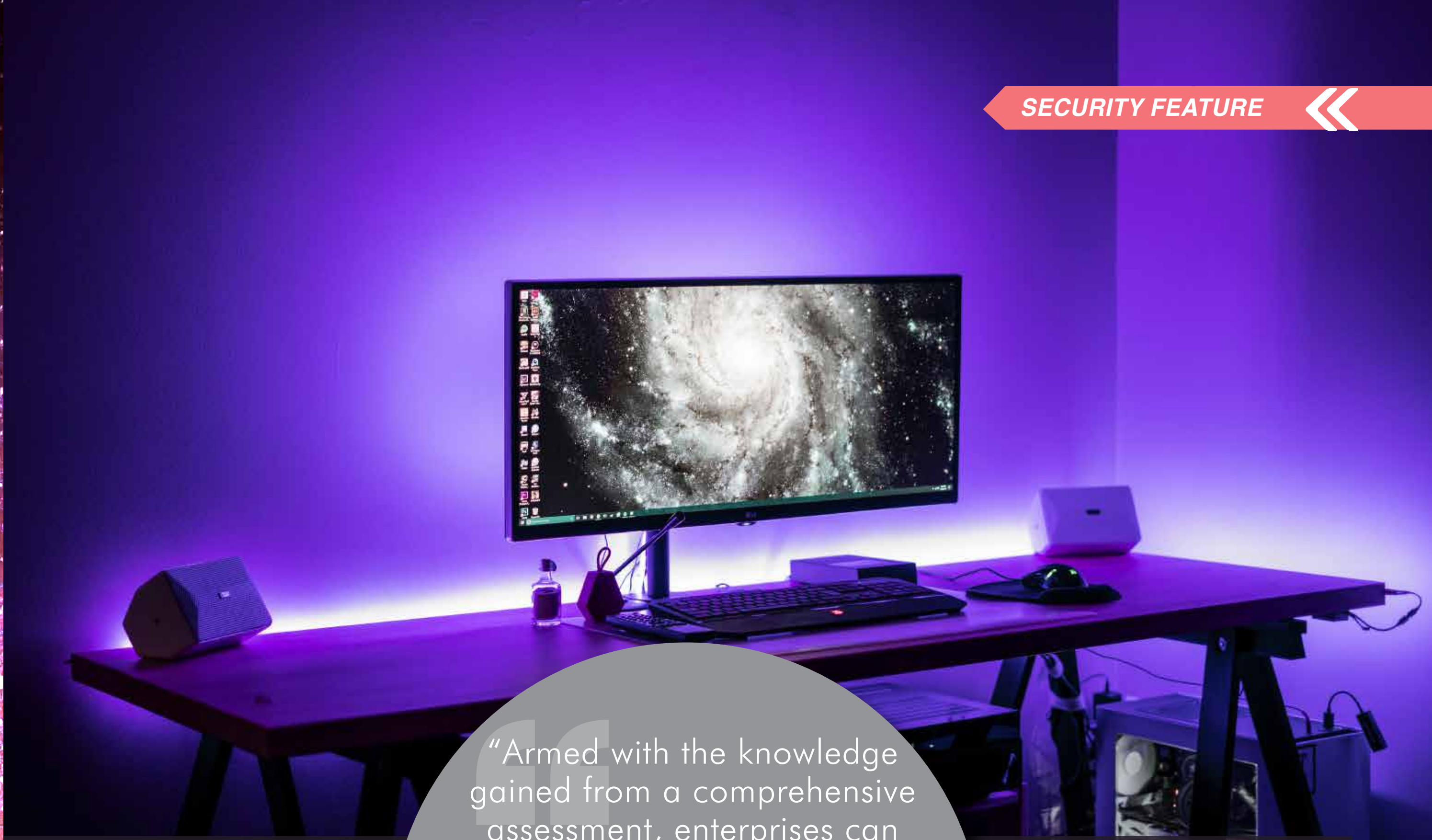
This approach, is the equivalent to treating each cyber security requirement that crops up as one tree in a vast forest of similar requirements. Businesses are dealing with each tree on its own, when they should consider the whole forest to navigate it properly.

As the old saying goes, "They can't see the forest for the trees."

The Cyber Security Transplant

Many of today's businesses function on systems and processes that were created before rapid digitisation and were designed without taking those implications into account.

The most common approach to addressing a businesses' cyber security needs is to supplement their existing systems and processes with cyber



security solutions. Since the transplant of added security functions and requirements surpasses the original design of many of these established processes, enterprises end up with unintended and less efficient results.

"Armed with the knowledge gained from a comprehensive assessment, enterprises can begin to craft a strategy for their organisation that takes into account the whole and not just its disparate parts. A holistic approach provides the ability to visualise how the enterprise is implementing security from end to end."

Doing One Thing Well

Businesses tend to review their cyber security needs on an ad-hoc basis. Do we need a firewall to lock down network activity and secure our people? What about a patch management solution? Is there a vendor that can performs these functions the best and at a reasonable price?

This kind of implementation is not uncommon. It makes sense, is straightforward and there are clear results. There's no need to fix something that isn't broken, right?

While it is easy to fall into the practice of addressing requirements as they arise, there are drawbacks. It's difficult to gauge the effectiveness of these solutions based on the money spent.

Without an overarching strategy, spending occurs as need rises and does not take priorities into account. Additionally, there is a risk of deploying overly-complex systems. An enterprise that builds a cyber security program in this manner will eventually have disparate solutions. Any deficiencies in the system become difficult to diagnose as well.

The Knee-Jerk Response

In the two scenarios above, the spending is not only on point solutions, but also reactionary. This practice of reactionary spending is a short-sighted approach that lacks strategy and leads to difficulty in gauging cost-effectiveness of the solutions needed.

Enterprises need to deal with cyber security holistically, and not on an ad-hoc basis. Having a proper strategy in place means having the capability to deal with challenges as they crop up.

Cyber Security is Everything

The challenge in building an effective cyber security program is relatively new. Enterprises recognise the need for it but approach cyber security as a new business component to be added to existing business processes. This should not be the case. Cyber security changes the way business is done and affects all business processes. Cyber security is everything.

Businesses that hope to implement highly-effective cyber security strategies need to take a step back and consider their organisation as a whole and how cyber security affects every part of it.

Know Yourself

The foundation of a cyber security strategy is built from a thorough assessment to identify an enterprise's assets, critical business processes, and the threats to those assets and processes. A comprehensive accounting of these things will enable an accurate risk assessment to determine the priority in which those risks need to be addressed.

From the Ground-Up

Armed with the knowledge gained from a comprehensive assessment, enterprises can begin to craft a strategy for their organisation that takes into account the whole and not just its disparate parts. A holistic approach provides the ability to visualise how the enterprise is implementing security from end to end.

A strategy formulated in this manner will capture potential risks and prioritise them by severity, impact to the organisation, cost, opportunities for solution integration, and level of difficulty to implement. These decisions are complicated and involve serious consideration, but they could not even be considered without a full picture of an organisation's risk profile.

A holistic cyber security strategy contends that cyber security touches all facets of a business. Under this approach, business processes would generally need to be re-designed with cyber security considerations integrated at the foundational level. This means designing a cyber security strategy from the ground-up with the ability for integration into new business processes and scalability as opposed to deploying solutions that are to be grafted onto existing business processes.

An overarching, comprehensive cyber security strategy also allows for the design of platforms that consist of integrated solutions, instead of point solutions. This will provide an overview of cyber security requirements that will enable advanced, forward-thinking spending strategies.

> *"Even for organisations where cyber security is not a priority, cyber security is becoming an area of deep concern in boardrooms. As we delve deeper into the 21st century, enterprises that have been operating successfully for years and even decades with very little thought to digitisation, let alone cyber security, are scrambling to address the challenges of a cyber space full of threats."*

The Forest Emerges

With the adoption of a holistic method, enterprises become secure by design and not by necessity. Enterprises move from a fear-based approach in cyber security and instead begin an approach that is risk-based. Decisions are no longer tactical and short sighted. They become strategic and insightful. Spending is no longer reactive. It becomes proactive and anticipatory.

With this new way of thinking, enterprises can begin to see the forest through the trees. SST

E-Commerce Requires Beefed Up Cyber Security to Function Well

By Samantha Cruz, Cyber Operations Researcher

In an increasingly interconnected world, online shopping and electronic transactions have now transcended its innovation status to become part of our daily lives. Its ease of use and convenience, can also mean significant security risks since sensitive information and personal data are routinely shared among business owners and shoppers.

Some these security risks include the following:

Financial Data Theft/Fraud

Many attackers target personal information such as names, addresses and credit card numbers. This allows them to make purchases online using someone else's payment information. One method being used is called pharming or using fraudulent websites to manipulate people into giving out their credentials.

Another more effective and insidious method is deliberately targeting specific users and manipulating them into giving their personal information (also known as spear phishing). Other exploits used to steal financial information include, but are not limited to: SQL Injection, Cross-Site Scripting, Path Traversal, Session Hijacking, and Drive-by Downloading

Distributed Denial of Service (DDOS) Attacks

A Denial of Service attack's aim is to take down e-commerce sites

"A Denial of Service attack's aim is to take down e-commerce sites by flooding them with requests. This kind of attack overloads the e-commerce site to the point where it can't handle anymore requests, making the service slow down or even go offline.Slow service for an e-commerce site means loss of potential revenue and massive impact to brand reputation."

by flooding them with requests. This kind of attack overloads the e-commerce site to the point where it can't handle anymore requests, making the service slow down or even go offline.Slow service for an e-commerce site means loss of potential revenue and massive impact to brand reputation.

Man in the Middle Attack

Man in the Middle attacks do exactly what they say—the attacker eavesdropping or intercepting the user's (in this case, the online shopper's) connection with the website. Even with Secure Sockets Layer (SSL)/Transport Layer Security (TLS) in place, there are still ways attackers can trick the browser to gain access to the plain text data.

Effects of A Security Breach for An E-Commerce Site

If such an attacker manages to compromise an e-commerce site, the following can happen:

Loss Of Revenue

The first, most obvious effect of a security breach is loss of income. Small businesses shell out an average of $38,000 to recover from a single data breach in direct expenses alone. On top of that, a company that experiences a security breach can also be held accountable for not following data protection policies, leading to hefty fines that can lead to a business's insolvency.

Damage to Brand Reputation

Apart from the direct loss of sales due to site unavailability (due to a DDoS attack, for example), losses of sales can also be due to customers walking (or in this case, browsing) away from the shop in favour of other shops without such security breaches. Losing customers' and stakeholders' trust is the most harmful impact of a security breach.

People will not do business with a breached company, plain and simple.

Even if the company is eventually able to recover the financial losses, the impact on the company's reputation would be a scar that would take a significant amount of time to fade. That is, if it even fades at all.

Intellectual Property Theft/Damage

Another impact of a security breach is theft and damage to intellectual property like trade secrets, blueprints, and anything else that gives a company their competitive advantage. This can mean missing out on expanding the business since the company can no longer fully implement new and innovative ideas brewing in the pipeline.

How to Protect E-Commerce Sites

The good news is there are ways e-commerce shop owners can protect their websites, their customers, and their data:

"Hackers and cybercriminals only get smarter and more sophisticated with each passing year. Therefore, the onus is on business owners to make security a priority. While a cybersecurity endeavour takes a lot of time and resources, the upfront cost is still lower than the potential losses and is a worthwhile investment for all e-commerce setups."

Research on the e-commerce platform and payment gateway the e-commerce business runs on to ensure it complies with information security standards.

Make sure the platform is compliant with the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS is an information security standard defined to control how credit and debit card information is handled. To determine if the e-commerce platform is compliant, refer to Visa and Mastercard's compliant service provider lists.

If you plan to implement your own platform using open-source platforms like Magento, then the responsibility is on the shop owner to implement security measures.

Ensure that your shop is PCI-compliant and other basic security measures are in place.

Make sure the entire site (not just the payment area) uses HTTPS and do keep the SSL certificate updated.

The certificate creates a secure connection between the user and the server. Otherwise, the data is easily accessible and readable by anyone. Contact your hosting provider if the shop is not hosted via HTTPS.

Only store customer data that is needed and make regular backups of them. Conduct a vulnerability scan on the online shop.

Even with security measures in place, it is possible that the site is still vulnerable from threats that are not obvious to the end user. This is where a web scanner comes in. Web scanner scans web applications for known vulnerabilities by spidering through links and ignoring pages linked outside the target domain.

Security Is Number One From Day One

Hackers and cybercriminals only get smarter and more sophisticated with each passing year. Therefore, the onus is on business owners to make security a priority. While a cybersecurity endeavour takes a lot of time and resources, the upfront cost is still lower than the potential losses and is a worthwhile investment for all e-commerce setups. SST

Predictions for Fintech: Balancing Hype with Realism in 2018

By Genady Chabranov, Director, Financial Technology Innovation at Hitachi Vantara

VIEWING EXCITING ADVANCES THROUGH THE LENS OF PURE PRAGMATISM

The vast and constantly shifting ocean of Fintech, and all that it encompasses, has seen ripples and undercurrents become indomitable swells in terms of the changes it has brought upon us recently.

As our understanding of the opportunities and challenged develops, I feel that a pragmatic approach offers us the best lens through which to view the movements and progression of the Fintech sector.

When talking to customers in 2017, I've noticed that conversations have moved from technology-centric to solution-centric. I believe this is a result of a wider understanding of Fintech and its practical implications, as well as the businesses, technologies and methodologies it touches. In this article, I will outline some of those conversations and the way I expect them to impact the sector in 2018.

Meet Customer Needs in Digital Transformation

Customers need solutions, which work well for them, that are simple to understand, and which are delivered quickly. The ability of Financial Services firms to provide personalised and frictionless service - anytime, anywhere - via multiple channels is going to be flavor of the year in 2018; this is exactly how we build in competitive advantage, show real leadership, and a permanent willingness to improve.

We are seeing banks move away from paper and analogue, and focusing increasingly on digital transformation. That's all fine of course, but they need a robust digital architecture with slick and reliable processes for this to actually happen. This in and of itself is fascinating to me, as I think I first heard the term 'go paperless' in 1998...

> "Analytics is especially interesting because, among other things, it directly transforms video data into competitive insights. Cameras are everywhere these days and have now become Internet of Things (IoT) sensors which can provide real-time intel. But to make the most of this value, organisations need an analytics solution. "

If the aim is to get closer to what customers want and accelerate digital transformation, then success requires a new template, model or approach that supports rapid change. We can bridge between traditional operations and agile innovation by centering ourselves on the critical enabler of digital transformation – Data - in all of its diverse expressions.

Operations like form filling and digital signature capturing allow banks to capture and analyze information faster and use advanced analytics to improve the overall customer experience.

Analytics is especially interesting because, among other things, it directly transforms video data into competitive insights. Cameras are everywhere these days and have now become Internet of Things (IoT) sensors which can provide real-time intel. But to make the most of this value, organisations need an analytics solution.

Exploring the Possibilities of Developed AI

In 2017, we saw machine learning playing a major role in creating personalised products, and in 2018 I expect to see the rapid development of solutions based on artificial intelligence.

Although the technology is still in its early stages, we are already seeing multiple AI use cases, for example better customer targeting and segmentation or the automation of processes such as loan underwriting or chat bots.

AI has also been a focus for Vantara featuring107 years of experience in operational tech and 58 years in IT that we combine in the smart IoT platform we call Lumada. Advanced analytics and machine learning are packaged into solution cores to solve business problems and help companies embrace the benefits of real-time optimisation and AI.

Pentaho, a Hitachi Group Company, announced earlier this year it had created orchestration capabilities that streamline the entire machine learning workflow and enable teams of data scientists, engineers and analysts to train, tune, test and deploy predictive models. Pentaho's Data Integration and Analytics platform ends the 'gridlock' associated with machine learning by enabling smooth team collaboration, maximising limited data science resources and putting predictive models to work on big data faster - regardless of use case, industry or language. So just think of the AI possibilities this could bring to Fintech in 2018!

Protection and Governance Become Paramount

Data governance and protection will be another key trend. Customers are now willing to share more information to receive more personalised services. However, ensuring protection of this data is often very challenging, since it is siloed and often unstructured.

Many large financial institutions are now working on centralising information to gain a holistic view of their data and processes. As a result, access control is becoming much tighter, and will become even more so in 2018.

"Data governance and protection will be another key trend. Customers are now willing to share more information to receive more personalised services. However, ensuring protection of this data is often very challenging, since it is siloed and often unstructured."

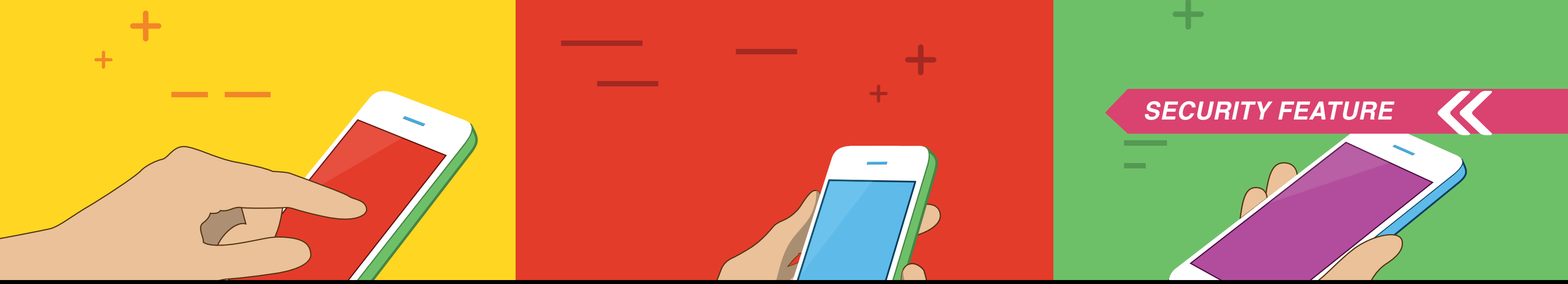
Companies need to focus on meeting governance and regulatory compliance rules and gaining absolute control of corporate data organisation-wide. These solutions securely automate discovery, extraction, classification, enrichment and categorisation across any data landscape. The aim is streamlined compliance, again with customer-centricity at its heart.

When it comes to Data Protection, my approach is "get it done yesterday". Old-school data protection has officially been disrupted and one only has to think about the companies who have become massive news stories for all the wrong reasons to see why.

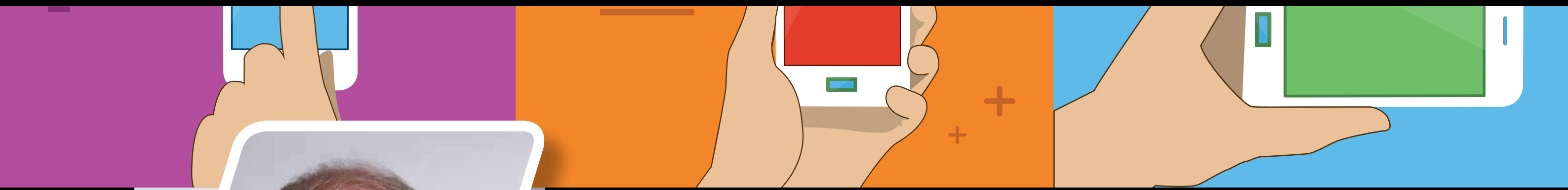
To become truly secure, companies need to focus on orchestrating backup, business continuity and disaster recovery within business-defined workflows, working to simplify a client's recovery challenges via a single unified platform; cutting cost, complexity and risk to meet the service-level requirements with advanced data management and protection techniques.

With these three pragmatic and methodological approaches, we can begin to get our heads around the challenges facing the Fintech industry - both now and in the future. We can also put a brave foot forward, and hopefully soon walk quickly in step with a fast-changing environment and therein lies the opportunity.

For more information, please visit: www.fintechnews.sg/tag/hitachi SST



THE GROWING POPULARITY OF SMART PHONES AS ACCESS CONTROL CREDENTIALS



►► *By Scott Lindley, General Manager, Farpointe Data*

Scott Lindley is a 25-plus year veteran of the contactless card access control industry. He is the General Manager of Farpointe Data, the leading OEM for cards and readers.

Smartphones fulfill many needs, including telephone, camera, navigation, music, video, clock, news, calculator, email, Internet, gaming, contacts, and more. Security professionals creating access control systems need to be aware that 95+ percent of all adults 18-44 years own smart phones. Plus, 69 percent of the entire population already uses smart phones. That's babies through seniors. And, the average smart phone user touches their device 2,617 times a day ((Dscout Research)!

Thus, practically anyone using an access control system already carries a smart phone. Another way to look at it is that every smart phone user, or almost everybody, could now easily download an access control credential.

Mobile credentials are smart phone-based versions of traditional RFID cards and tags. Mobile credentials make it possible for smartphones, such as the Apple iPhone® and the range of Google Android® devices, to be used as an electronic access control credential.

No longer will people need various physical credentials to move throughout a facility. Instead, a person's iPhone or Android smart phone, which they carry with them wherever they go, will have the credentials they need to enter into any authorised access system. In fact, such a system can reach beyond the facility into their homes, their automobiles or at the gym.

"Mobile has already disrupted so much in both our personal lives and the enterprise, but we are still tapping an old school badge on a door access reader," David Anthony Mahdi, research director at Gartner Research says. "It's a dichotomy. On one side we are doing all these amazing things with our phones but then we are still using 20-plus year old technology to get into our buildings."

Referred to as mobile or soft, smart phone based access control credentials are another version of traditional RFID cards and tags, joining proximity and smart card credentials to support a user as she moves about a secured facility. Gartner suggests that by 2020, 20 percent of organizations will use mobile credentials for physical access in place of traditional ID cards. Soft credentials provide several advantages over hard credentials. They are more convenient, less expensive and more secure. This is true for both end users and installers.

They are more convenient because the user already has his credentials and already carries it with him wherever he goes. Credentials can be delivered to the end user in either paper or electronic form, such as via email or text. The dealer has nothing to inventory and nothing to ship. Likewise, the user sponsor has nothing to store, nothing to lose and faces no physical replacement hassles. Cost are lowered as nobody must undertake "1sy-2sy" replacement orders.

Original soft access control systems are already being used by innovators, approximately five percent of users, according to Gartner. There were the typical drawbacks with a new technology. Before they switched to soft credentials, the next wave of users have requested smart phone solutions that eliminate many of the frustrations that they discovered with their original smart phone apps and hardware, the main one being complicated implementation practices. The newer solutions provide an easier way to distribute credentials with features that allow the user to register only once and need no other portal accounts or activation features. By removing these additional information disclosures, vendors eliminated privacy concerns that have been slowing down acceptance of mobile access systems.

One additional concern held back some buyers. What if the baby boomers at our facility don't have a smart phone? Problem solved. Just be sure that your soft credential reader can also use a smart card.

Secure!

Many companies still perceive that they are safer with a card, Gartner's Mahdi notes, but if done correctly, the mobile can be a far more secure option with many more features to be leveraged. Handsets deliver biometric capture and comparison as well as an array of communication capabilities from cellular and Wi-Fi to Bluetooth LE and NFC, he adds.

Bottom line - both Bluetooth and NFC credentials are safer than hard credentials. Read range difference yields a very practical result from a security aspect. A Bluetooth reader can be installed on the secure side of the door while NFC must be mounted on the unsecured side.

As far as security goes, the soft credential, by definition, is already a multi-factor solution. Mobile credentials remain protected behind a smart phone's security parameters, such as biometrics and PINs. Once a biometric, PIN or password is entered to access the phone, the user automatically has set up 2-factor access control verification - what you know and what you have or what you have and a second form of what you have.

To emphasise, one cannot have access to the credential without having access to the phone. If the phone doesn't work, the credential doesn't work. The credential works just like any other app on the phone. The phone must be "on."

Leading readers additionally use AES encryption when transferring data. Since the Certified Common Criteria EAS5+ Computer Interface Standard provides increased hardware cybersecurity, these readers resist skimming, eavesdropping and replay attacks. With the U.S. Federal Trade Commission (FTC), among others, now holding the business community responsible for implementing good cybersecurity practices, such security has become an increasingly important consideration.

If the new system leverages the Security Industry Association's (SIA) Open Supervised Device Protocol (OSDP), it also will interface easily with control panels or other security management systems, fostering interoperability among security devices. Likewise, check if the new soft system requires the disclosure of any sensitive end-user personal data. All that should be needed to activate newer systems is the phone number of the smart phone.

"No longer will people need various physical credentials to move throughout a facility. Instead, a person's iPhone or Android smart phone, which they carry with them wherever they go, will have the credentials they need to enter into any authorised access system. In fact, such a system can reach beyond the facility into their homes, their automobiles or at the gym."

Lastly, once a mobile credential is installed on a smartphone, it cannot be re-installed on another smart phone. Think of a soft credential as being securely linked to a smart phone. If a smart phone is lost, damaged or stolen, the process should be the same as with a traditional physical access credential. It should be immediately deactivated in the access control management software - with a new credential issued as a replacement.

Installing Soft Credentials Is So Much Easier

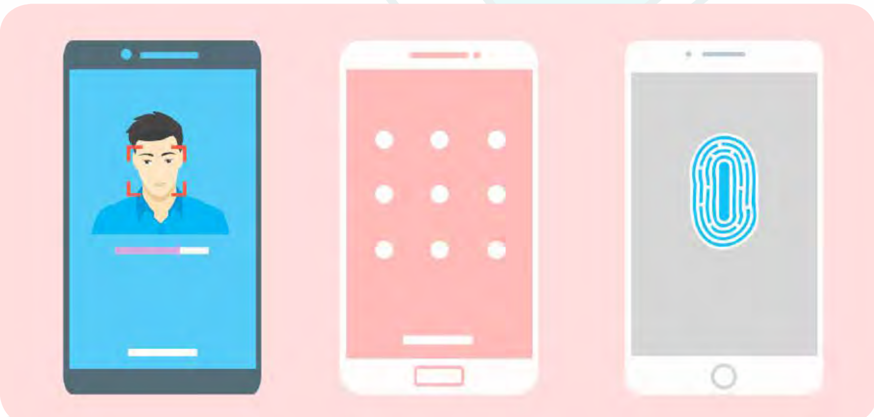
Smart phone credentials are sold in the same manner as traditional 125-kHz proximity or 13.56-MHz smart cards - from the existing OEM to the dealer to the end users. For the dealer, smart phone credentials will be more convenient, less expensive and more secure. They can be delivered in person or electronically. They are quicker to bill with nothing to inventory or to be stolen. Also, in most cases, soft credentials can be integrated into an existing access control system. Distribution can also be via independent access control software.

There are two types of software. First is the Wallet Application, a free software that is downloadable from the Apple App Store or the Google Play Store. Its purpose is to hold the access control credentials. Typically, the Mobile Wallet App will store as many credentials as you will want, all at one time.

The Mobile Access Credentials are the individual credentials needed to gain access. Each credential can be programmed to work with a specific access control system. This means that, yes, a single smart phone, holding multiple access credentials, can be used to gain access on multiple access systems. No longer will users be required to carry individual multiple hard credentials. The employee just carries her smart phone which has them all within it.

"The Mobile Access Credentials are the individual credentials needed to gain access. Each credential can be programmed to work with a specific access control system. This means that, yes, a single smart phone, holding multiple access credentials, can be used to gain access on multiple access systems. No longer will users be required to carry individual multiple hard credentials. The employee just carries her smart phone which has them all within it."

Smart phone credentials deploy so much faster than hard credentials. To install a mobile credential, a user needs to first have the Wallet App installed on a supported smart phone. Next, you launch the App and select the "Add" button, indicating that you would like to load a new credential. A Registration Key Certificate is provided for each credential ordered. Now, enter the unique 16-character Key from the Certificate and tap "Submit." Once successfully registered, the new mobile credential will appear in the Wallet App ready for use. From that point on, the user simply holds their smart phone up to reader when they approach it.



Why Multiple Credentials Are Emphasised with Smart Phone Access Control

The simple reason is that this is the future. Already, we've discussed access control at the front door, the parking gate and for the data system. But, at lunch, soft credential would also be available at the cafeteria or the vending machines. Students could check out books while machinists select the tools they need. They become a photo ID at the club. All are separate applications with their own access control systems.

Thus, a Mobile Wallet App will normally store many credentials on a smart phone at one time. The actual quantity is dynamic and is related to the memory specifications and internal storage space available on each individual smart phone and, more opportunities are on the way. How about using your smart phone as an intelligent key for your car? Want to know where your child is driving, how fast or if he added gas or oil? How about using it to access your gym, automatically synch to a piece of equipment or analyze the effectiveness of your workout? Forget all those other tags and cards. Your smart phone will become the passport to all aspects of your life from work to home to avocations. At a fraction of the investment you have in hard credentials, secure soft, digital credentials are all you need.

The Hard Fact about Soft Credentials

Soft, mobile, smart phone based access control credentials are inevitable. Every security professional needs to get on board. SST

SMART CITY SURVEY RESULTS DEMONSTRATE THAT GOVERNMENTS NEED TO BE SMARTER ABOUT KEEPING CITIES SAFE

►► *By Keith Roscarel*

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 urbanized 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 reports estimates that smart cities accounted for more than 1.1 billion Internet of Things (IoT) items in 2015, rising to 9.7 billion by 2020.

The question that needs to be answered is can smart cities be safer places for people to live and work? And what role does the advancement of technology and IoT have to play in delivering public safety?

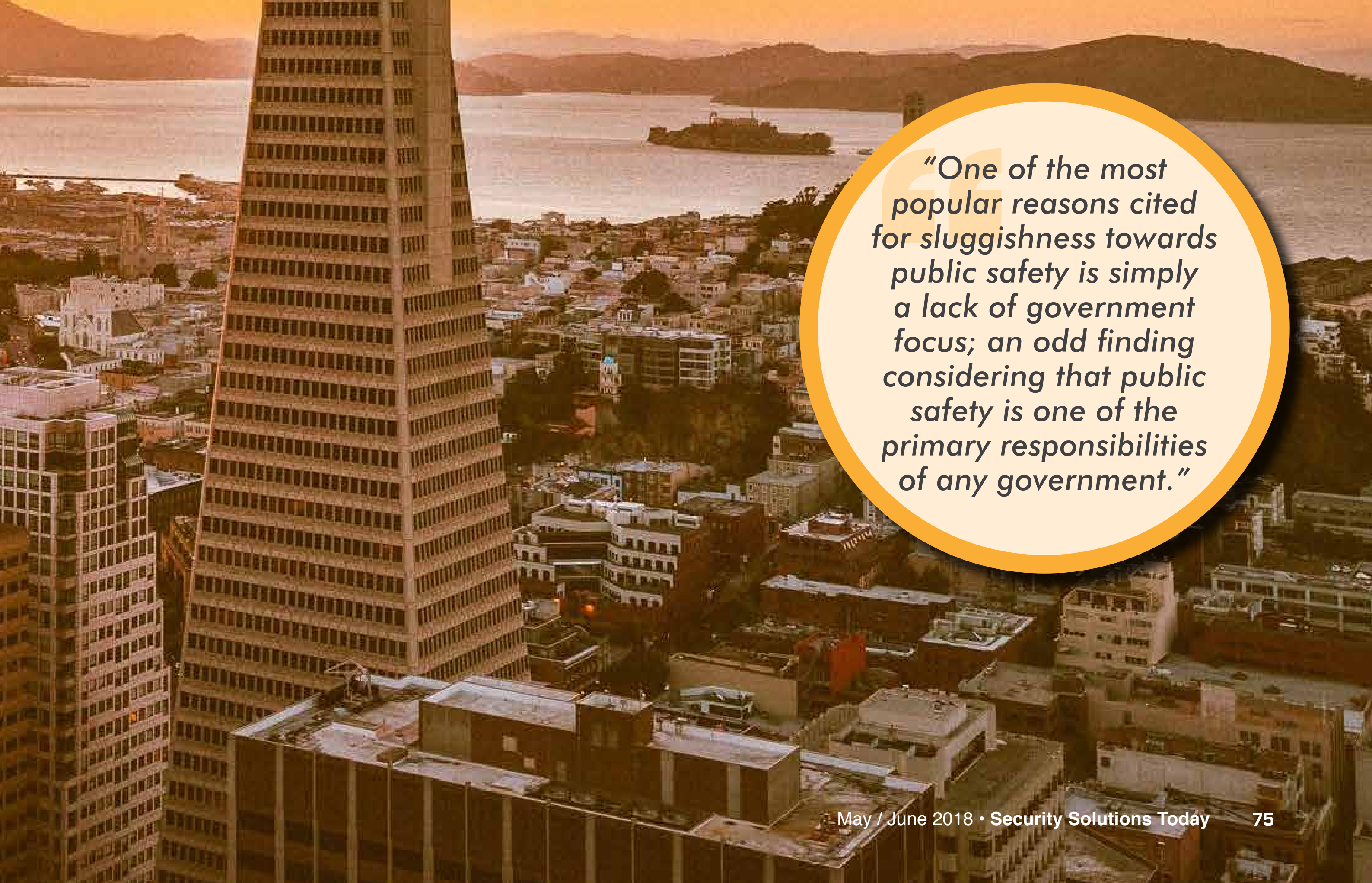
To find the answers, Hitachi conducted a survey of delegates at the Safe Cities Asia conference in Singapore. The event was attended by city government representatives, agencies and key municipal leaders from Asia Pacific, who discussed public security and safety challenges.

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



> *"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."*

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 realize 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.

"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 crime hot spots."

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 crime hot spots.

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. SST

SHRINKING THE CYBER ATTACK SURFACE BY HARDENING PHYSICAL SECURITY SYSTEMS

►► *By Viakoo*

If the data isn't already at hand, ask your IT manager how often someone tries to compromise your website or information network. Chances are, it's in the range of several hundred times each and every day. For the largest companies and most active websites, the number can reach 100,000. That is on average, more than once every second.

If these numbers are not sobering, also consider that datacenters and IT equipment is not where hackers are typically starting their attacks. All too often, it's ancillary systems like HVAC, physical security, and others that provide welcoming points of entry to a corporate network. These systems interconnect with others in such a way that there may be additional vulnerabilities that are not obvious to your IT teams. Attackers are aware of these vulnerabilities, and working quickly to exploit them and gain access to information networks through the relatively unprotected physical security systems.

Understanding the issues of potential vulnerabilities in your physical security systems' security and discussing hardening methods that can be employed to bolster your defenses and ensuring that countermeasures are in place, is a matter of some urgency. You might have had a dozen cyber-breach attempts, or more, in the time it took to read this introduction.

Physical Security System Vulnerabilities and Digital Systems Provide Benefits and Risks

In recent years, video surveillance systems moved towards digital formats and IP connections, and in 2014, digital security cameras first outsold analog cameras. Digital systems provide key advantages for users – for example, many can now provide basic analytics functions at the edge, and can store video marked with metadata to support enhanced searching, direct access, and other advanced functions. In a similar vein, access control systems have also become digital, providing increased intelligence and more complex advanced functions including multifactor verification and behavioral analytics, among others.

Importantly, the other big advantage of digital physical security systems from the user point of view is the ability to interconnect them with IT, identity, attendance, and other systems, and to connect them to the internet-based services. Interconnection between systems provides for additional management and information functionality. For example, access to sensitive IT resources can be made dependent on successful multifactor verification in the access control system, within the expected working hours in accord with HR databases. That is, someone could be granted access to sensitive information only within their normal working hours, and after they were confirmed to arrive at the office that day. In theory, for example, this would prevent a coworker from using someone else's password after normal working hours to access unauthorised documents – a level of control that was not possible without these interconnected digital systems.

Connecting these systems over the internet infrastructure enables managers to access information and take actions remotely an enormous benefit that is almost taken for granted in today's mobile environment. The trouble with these developments is that by making it possible for managers to access their systems from anywhere, and interconnecting them to allow for enhanced management and information functionality, if not architected securely, companies can simultaneously expose themselves to hackers and intruders.

Today, many physical security system elements are networked, making them reachable through a network, and also, if not architected securely, can make each of them a possible entry point for attackers. These vulnerable points include networked video cameras and video recorders, switches and transmission devices, access controllers, card readers, and keypads, badge printers, among many others thanks to the IoT.

Vulnerability is 'Baked In'

Moreover, the nature and the reality of the situation often makes addressing these vulnerabilities more difficult. For example, every installed system is made up of elements from multiple suppliers and, few companies installed all their systems at the same time; instead, systems were installed, upgraded, expanded, and replaced over time, as needed. As a result of both of these factors, essentially all installed systems are both "multi-vendor" and "multi- generational" – a situation that cannot be changed under any reasonable circumstances. Any solution that would strive to improve cyber-resilience for such systems would have to span across all networked devices and account for wide ranges of functionality, scale, and complexity.

Hardening Physical Security Systems

As challenging as the situation seems, companies have little choice other than to put up a fight when it comes to blocking potential cyber attackers. Fortunately, there are straightforward steps that can be taken to harden

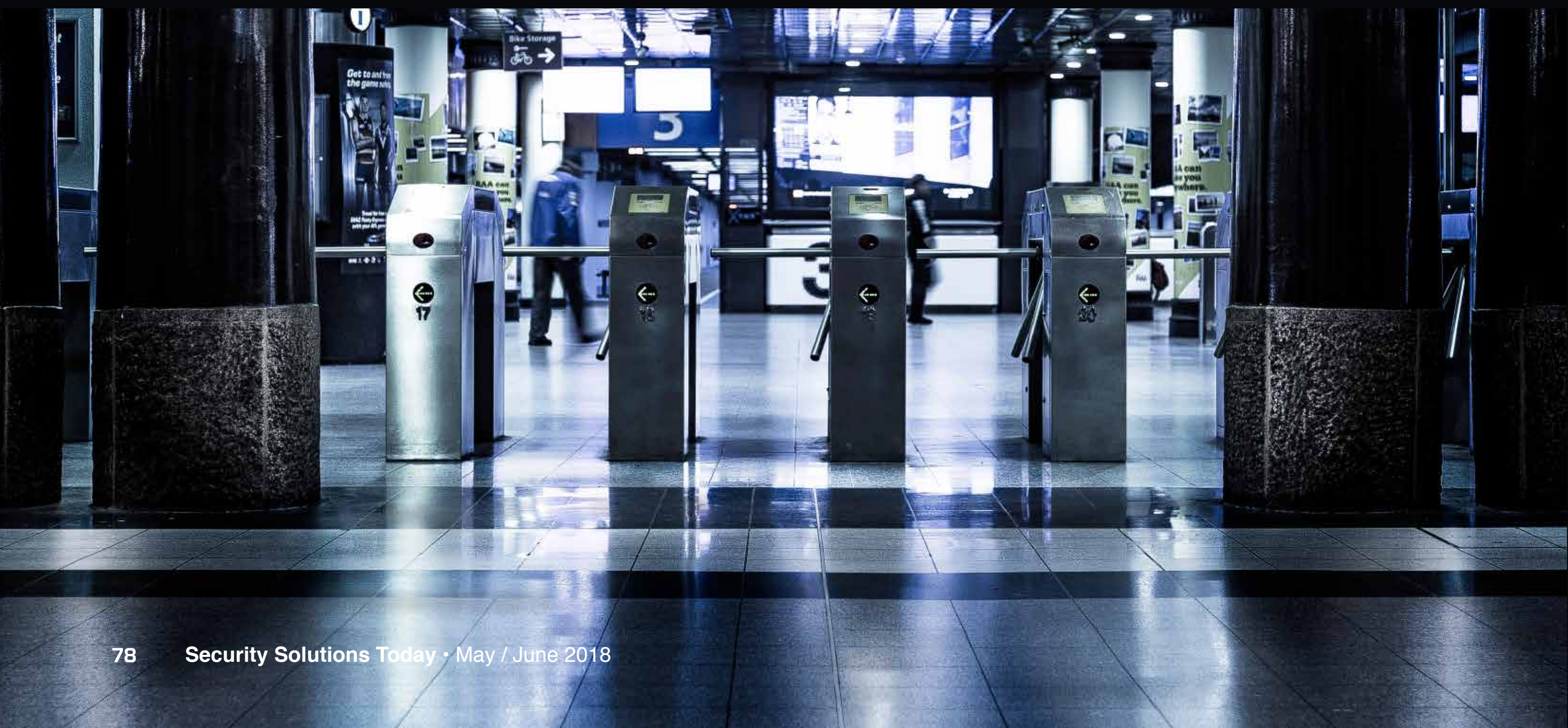
"Today, many physical security system elements are networked, making them reachable through a network, and also, if not architected securely, can make each of them a possible entry point for attackers. These vulnerable points include networked video cameras and video recorders, switches and transmission devices, access controllers, card readers, and keypads, badge printers, among many others thanks to the IoT."

interconnected and networked systems, reducing vulnerabilities and the likelihood of a successful attack. These recommendations are based on an extensive set of cybersecurity best practices, as well as the recommendations of applicable standards bodies.

For convenience and clarity, the recommendations are organised by type, not necessarily by priority or importance. Evaluate the specifics of your circumstances to determine which steps are needed and in what order to prioritise them to support your business needs.

Staff

Provide ongoing security awareness and education as most vulnerabilities are actually from within an organisation, whether accidental or intentional.



Software

Ensure that all software throughout the system is updated at all times, including device firmware. Consider automating the checking and updating process with automated authenticity verification safeguards.

Passwords

Establish and enforce a password management policy. No networked devices should continue to use default passwords provided by the manufacturer.

Current best practices on passwords emphasises length as a major security determinant. Longer is better. Implementing periodic password changes will also greatly enhance security throughout the systems. Failed login attempts, either by user names or passwords, should be limited, investigated and locked out.

Privileges

Clearly define and determine the appropriate groups; differentiating between administrators, operators and users, and casual users and visitors. Each group should be assigned the system rights and privileges necessary for their assigned functions, and no more. VPN access should not be allowed for admin functions, diagnostics, or similar sensitive information or access. Rights and privileges should be reviewed and adjusted periodically.

Securely Architected Systems

Security systems can be securely architected so that they can have a low risk connection to the internet. Careful attention needs to be given to limit susceptibility to hacking attempts. Of course end points (cameras) and other access points, and links to information networks need to be programmatically managed to automatically determine all system elements and exactly what is connected to what.

Carefully curate all connections that support remote access. Wireless devices have vulnerabilities that must be managed as they could provide an easy gateway to physical security servers. Secure all wireless devices connected to corporate networks, including cameras, locks, printers, and modems so they cannot be accessed by unauthorised traffic. Implement logical separations for virtual local-area networks (VLANS) and access controls lists (ACLs) that instruct system elements to only allow access to specific authorised devices, and to deny all other requests.

> *"Many firms are short-handed when it comes to security. Many studies have reported on a global shortage of cybersecurity talent that is expected to continue. Automated system verification tools such as those provided by Viakoo provide a powerful alternative that can provide a more consistent and better detection/alerting function to detect all types of security-related issues. "*

Endpoint Connections (including cameras, badge readers, control panels, security- related servers and video recorders)

Hackers can gain access to the security network by plugging into a network cable that was installed to reach an external camera, or plugging into open USB ports on security endpoints. Port security can be used to protect against such connections by providing an additional layer of protection to restrict unauthorised devices from connecting to router or switch ports. Port security makes use of the hard-coded MAC address of the authorised device, which unlike an IP address, is difficult to change. If a device is connected to a switch or router that doesn't match the registered MAC address, then the system can block access to that device and raise an alarm for follow up.

Improving Cyber-Event Detection With Automation

Many firms are short-handed when it comes to security. Many studies have reported on a global shortage of cybersecurity talent that is expected to continue. Automated system verification tools such as those provided by Viakoo provide a powerful alternative that can provide a more consistent and better detection/alerting function to detect all types of security-related issues.

Automation can also check and verify that the installed firmware and software is current throughout physical security systems. The most powerful solution is to programmatically check the integrity of the video streams and stored video les themselves to be sure that the system is operating as intended and that the video records are being stored as designed.

Conclusion

Cybersecurity threats are a current real and present danger to any organisation with networked security operations. Hardening the organisation's physical security system is a good way to reduce the risks from cyber criminals because determined attackers know that the physical security systems generally have fewer cyber protections in place. The most powerful solution is an automated system to verify that surveillance video is being collected and stored as intended, so that immediate action can be taken in the case of gaps. Hackers are almost certainly trying to penetrate your corporate network right now. Don't wait for them to find a weakness, take action to harden your physical security network now. SST

10 SECURITY INDUSTRY TRENDS EXPLORED AT ISC WEST 2018

2018's Most Significant Emerging Threats and Business Opportunities of the Industry Covered at the Event

ISC West, sponsored by the Security Industry Association (SIA) is the largest converged security event of 2018, constantly evolving to educate security professionals on the tools and skills needed to protect against today's emerging cyber and physical security threats and the anticipated ones of tomorrow. This year's exhibition was held at the Sands Expo in Las Vegas, Nevada USA from 10 to 12 April 2018.

ISC Security Events is an iconic, 50-year-old brand that has its finger on the pulse of the integrated cyber-physical security industry, allowing it to seamlessly evolve to cover every emerging threat. Through its partnership with SIA, ISC West organised a comprehensive program for attendees from all industries, roles and functions across physical, IT and IoT security.

Booming Growth of the IoT

Both enterprise and consumer-connected solutions were major focuses at ISC West and were explored in-depth at the Connected Security Expo and the Connected Home areas. According to Gartner, businesses are predicted to represent more than half of overall IoT spending in 2017 (57 percent). Going into 2018, cross-industry devices, like those used in smart buildings (i.e., LED lighting and physical security systems) will drive this spending trend. The IoT is creating both challenges and capabilities for the physical security and risk management sectors. When implemented and properly secured, the IoT will provide predictive analytics, the ability to deliver a more personalised experience to users, and complete situational awareness from top to bottom.

Cyber Meets Physical Security

As the cyber and physical security sectors continue to merge, manufacturers are dealing with increasingly hostile and complex environments. To take security to the next level, manufacturers and systems integrators need to offer more

Going into 2018, cross-industry devices, like those used in smart buildings (i.e., LED lighting and physical security systems) will drive this spending trend. The IoT is creating both challenges and capabilities for the physical security and risk management sectors.

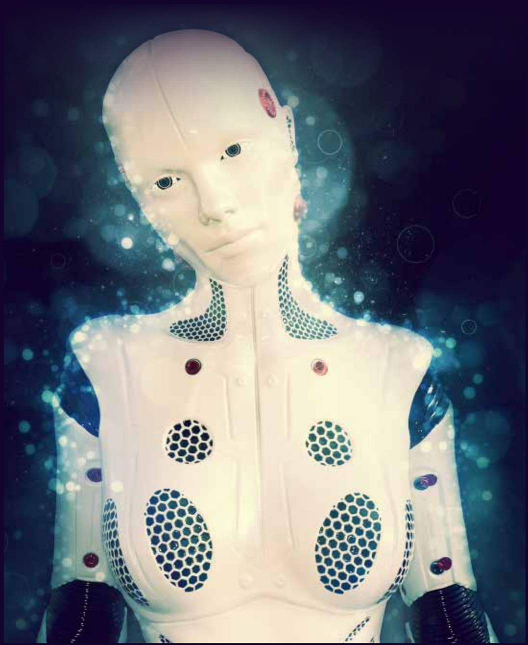
advanced cybersafeguards to protect network connected devices.

Security integrators are moving in the right direction and are beginning to offer cybersecurity as a service as they continue to grow their businesses from hardware-centric to solution-oriented models. And customers rightfully expect service providers to be their trusted advisors – however, integrators will only be able to deliver if they continue to evolve towards total convergence.

Accessing and Analysing Smart and Big Data

According to IDC, less than .5 percent of all data is ever analyzed and used, which is alarming considering all the buried insights that exist but aren't being leveraged. According to Lisa Roy, Vice President, Integration and Commercial Operations, Building Solutions-North America of Johnson Controls, "Big data is life changing in how we operate buildings and determining our future role. It's all about how to pull that information out that benefits the customer. Big data changes the way in which we service customers."

Augmented reality (AR), artificial intelligence (AI) and video analytics will continue to be important for acquiring insights, but physical security experts are already anticipating how Big Data will impact the industry beyond these technologies. With so much information available, security practitioners need to have a plan for the data they are collecting, as well as a realistic risk assessment of the exposure of this data to their companies and clients.



Evolution of Risk Management

Traditionally, the organisational process in security has been a siloed, single-lane approach. However, the most successful management models include all corporate stakeholders and possible sources of information to circumvent loss and reduce the potential for insider risk threats. We're heading in the right direction as risk management and planning has broadened to be more holistic, and collaboration between all stakeholders, beyond just within technology/security roles, is becoming increasingly prominent. However, this needs to happen even more, to become the norm, not an exception. As we look to innovative technologies that bring about new risks and considerations, such as drones, this coordinated approach becomes even more imperative. The Unmanned Security & Safety Expo @ ISC West further explored risk management for unmanned aerial and ground vehicles (UAVs, UGVs).

Transformation of the Channel

There's an ongoing, heightened transformation of the security installer and integrator business into everything as a service, with new models embracing interactive products and the DIY and self-installation markets. Unusual suspects from the IT sector have entered the security business, and traditional security monitoring companies are now offering DIY or self-install systems.

This transformation of the channel requires some changes. The traditional security provider must continue to change and focus on value-added services that heighten the customer experience, while delivering convenience and intelligence expected by their customers. From the end user's perspective, security executives are looking for security providers who can collaborate fully to address risks and assist not only with security and safety, but contribute to business continuity and promote a tangible return on investment.

Shakeup of the Status quo: Entrance of Entrepreneurial Buyers and Outsiders

Strategic acquirers are merging with traditional security manufacturers and installation companies to focus on data analytics, convergence and IoT. According to Jay Darfler, SVP, Emerging Markets and Innovation of ADT Security Services, "Disruption and innovation can come at you from a hundred different angles. You have to divide what your strengths and your core innovation to focus on."

The industry's biggest players are getting even bigger as new technologies and applications enter new markets, like residential, and even spill over into small-to-medium business

As the IoT and other disciplines continue to converge, social media will be part of the transformation of critical information resources. The next step for social media is deeper integration with mass notification and emergency communications—with the ability to disseminate specification information to individuals who may need to be evacuated or take shelter.

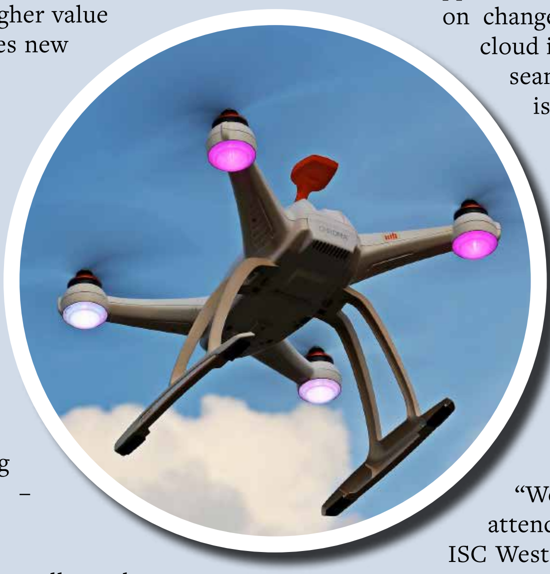
markets. However, there are challenges, and the longtime recurring monthly revenue (RMR) centric model is changing from hardware and project-based to income from service, maintenance and remote monitoring from cloud and interactive services and while service creates value, monetary values inevitably change. As this shift continues, norms that have been in place for decades are changing, too, including increased subscriber acquisition costs (SAC), decreased RMR margins, increased technology obsolescence, shorter product development cycles, no contracts, and interoperability.

Mobile Everything

Mobile technology is becoming synonymous with access identity and credentialing. Beyond the obvious consumer value, smartphones will be transformative within access control, enabling both cost reductions and end-user benefits. By itself, mobile credentials in access control is a strong value proposition, but mobile credentials are also able to provide an integrated and higher value system for the user while it promotes new services and revenue streams.

Control Through Cloud: Driving Greater Efficiencies and Promoting Managed Services

The global cloud computing service market is expanding exponentially. Growing connectivity, convergence and integration with IoT, mobile technology, and a wide range of applications and services is driving the shift towards cloud-hosting – including public, private and hybrid.



The cloud is an enabling technology. It allows the user greater access to managing their premises, and opens the door to new service options for solutions providers to offer. It gives them the opportunity to offer managed services and subsequent RMR that is highly attainable, providing inherent opportunities to add new revenue streams with the cloud's "always on, always accessible" model. With this, systems integrators can become total solutions providers that are reliably available 24/7, leading to greater confidence and customer satisfaction.

Integrating With Social Media

In law enforcement and emergency communications/operations, social media has become critical in identifying active shooters, criminal activities or other potential threats or disasters in real-time.

As the IoT and other disciplines continue to converge, social media will be part of the transformation of critical information resources. The next step for social media is deeper integration with mass notification and emergency communications—with the ability to disseminate specification information to individuals who may need to be evacuated or take shelter.

Emerging Connected Services: Consumers Want Convenience at Their Fingertips

Sensors embedded in a wide range of smart home devices and appliances will deliver near real-time analytics on changes within home environments. The cloud is a key component of this, providing seamless access and visibility. Visibility is especially important for service and maintenance of remote sites, reducing expensive site visits and labor costs – resulting in a better customer experience.

Security providers who can adapt with this changing landscape will prove invaluable to the commercial market, lowering their business costs in areas like energy management.

"We're laser-focused on providing attendees with all-inclusive education at ISC West, which is why we're thrilled to have SIA as our trusted partner," said Will Wise, Group Vice President of ISC Security Events. "These top 10 trends really hit on what was presented at the show. These themes impact nearly every type of attendee in some way, from government/enterprise security decision-makers and end-users, to integrators, installers and dealers. This year's show was designed to be the most educational and information-packed yet.

For more information, please visit: www.iscwest.com

Asian Securitex 2018
9-11 May 2018
Hong Kong Convention & Exhibition Centre

SECURITEX 2018 HIGHLIGHTS THE INNOVATIVE EDGE OF SECURITY TECHNOLOGY IN THE ASIAN MARKET

Build4Asia 2018 is the No.1 Tradeshow for the Building, Electrical Engineering and Security Industries in Hong Kong, which covers every facet of the construction industry from building materials and automation, smart city technologies to total surveillance system. Build4Asia is the ultimate B2B sourcing platform for companies to seek and widen their business opportunities. Securitex 2018 will be one of the segments featured that will feature security technologies. The 15th Asian International Security, Safety and Fire Protection Show & Conference will be strictly open to professional trade and business visitors. Featuring a wide range of innovative exhibitors, the show is reputed for being on the forefront of industry innovation, showcasing an array of cutting-edge technologies and solutions. There will also be a series of interactive forums, workshops and design galleries, further promoting industry networking as well as knowledge and the exchange of expertise.

This year, Securitex 2018 will comprise of various sectors in the ever-evolving security industry such as Electronic Article Surveillance (EAS), IP Security, Access Control, Surveillance Solutions and Lock Sales. In keeping up with the current digitalisation that the security industry is undergoing, there will also be sectors such as Intelligent Buildings, Information / Data Security, Biometrics and Home Automation Security Solutions or SMART home solutions which are currently trending as a hot topic with more and more companies jumping on the SMART wagon.

Featuring hundreds of exhibitors, the show that is held once every 2 years offers an unrivalled platform for industry suppliers for a wide range of high quality products as well as cutting-edge technologies and solutions. The show will most definitely serve as an excellent platform for professionals in a multitude of security industries such as Safety and Security Management, law enforcement and public safety, system integrators, IT management, distributors and even government to network and explore the latest developments in the security industry.

For more information, please visit: www.build4asia.com SST

ConnecTechAsia 2018
26 – 28 June 2018
Marina Bay Sands & Suntec Singapore

NEW MEGA TECHNOLOGY EVENT CONNECTECHASIA ADDRESSES ROLE OF ACCELERATED DIGITAL CHANGE IN ASIA'S GROWING ECONOMY

Singapore – ConnecTechAsia, combining the strengths of industry stalwarts CommunicAsia, BroadcastAsia, and newly launched NXTAsia, is the region's latest Mega Technology event, and will stage its inaugural edition from 26-28 June 2018, in Singapore.

With legacy events CommunicAsia and BroadcastAsia having served the telecommunications and broadcast media sectors respectively for nearly 40 years, the new NXTAsia builds upon this to bring new technologies that are shaping Asia's increasingly innovation-driven economy. With the advent of the Industry 4.0, ConnecTechAsia will present a holistic ecosystem of infrastructure, technology, and services that businesses and governments in Asia need to thrive in this new era.

"As Asia pursues digital transformation at an accelerated pace, it is critical that the event evolves alongside the dramatic shifts happening in the spaces we serve," said Mr Victor Wong, Project Director, UBM, organiser of ConnecTechAsia. "The new event reflects the pulse of Asia today, and is the only business platform covering the converging ecosystems of communications, broadcasting and emerging technologies connecting the physical and digital worlds."

At NXTAsia, industry professionals will catch the newest innovations and thought-leadership in areas such as Artificial Intelligence (AI), Augmented and Virtual Reality (AR/VR), Cyber Security, IoT, Robotics, Cloud and Data among others. NXTAsia will host promising start-ups, and the Singapore-leg of renowned start-up competition SeedStars, at tech showcase Disrupt+.

CommunicAsia, Asia's most established international industry event for the telecommunications sector, will focus on Network Infrastructure/FTTx, satellite communications and telecom software and services - the latest technologies to help companies and governments in Asia prepare for the coming of 5G and maintain a competitive edge in the communications and digital world.

"The new event reflects the pulse of Asia today, and is the only business platform covering the converging ecosystems of communications, broadcasting and emerging technologies connecting the physical and digital worlds."

With on-demand and streaming services surging in popularity, BroadcastAsia will shine a spotlight on the future of broadcasting, exploring how we have consumed news and entertainment over the past decade, and the challenges and opportunities this creates for traditional broadcasters and OTT players. BroadcastAsia will highlight technologies that are reshaping the value chain, such as the latest innovations in UHD/HDR, IP Broadcasting, Live Production, Content Media Security, OTT and Alternative Content Platforms.

ConnecTechAsia Summit - Digital Business Transformation

The ConnecTechAsia Summit this year centres on Digital Business Transformation, covering the hottest trends across ICT, broadcasting industries and enterprises to enable a digitalised future. The three-day summit comprises three tracks NetworkComms, BroadcastMedia and EmergingTech – that will drive business growth and sustainability.

5G, Network Virtualisation, Satellite Communications and Network Slicing will be the main topics in the NetworkComms track, while The Future of Television, Monetisation Strategies, Social Video, IP Broadcasting, 4K, AI and Immersive technologies for broadcasting will feature in the BroadcastMedia track. Topics of the EmergingTech track will include: Artificial Intelligence/Machine Learning, Blockchain Technology, Cybersecurity, IoT, Data Analytics, Seamless Commerce/Digital Payments, Connected Industries, IoT, Augmented, Virtual and Mixed Reality, and Smart Cities.

Key speakers include:

- Professor Howard Michel, CTO, UBTech
- Jassem Nasser, Chief Strategy Officer, Thuraya Telecommunications Company
- Ajey Gore, Group Chief Technology Officer, Go-Jek
- Geert Warlop, Chief Operating Officer, TrueMoney International
- Rene Werner, Chief Customer Service & Customer Experience Officer, Celcom Axiata Berhad
- Leah Camilla R. Besa-Jimenez, Chief Data Privacy Officer, PLDT
- Ian Yip, Chief Technology Officer - Asia Pacific, McAfee
- Arvind Mathur, Chief Information Technology Officer, Prudential Assurance
- Bill Chang, Chief Executive Officer - Group Enterprise , Singtel
- Parminder Singh, Chief Commercial and Digital Officer, Mediacorp
- Sanjay Aurora, Managing Director - Asia Pacific, Darktrace

"Presenting a holistic ecosystem of digital convergence and a platform for the discovery and understanding of new frontiers of innovation to elevate the global standing of Asian business and governments sits at the heart of what ConnecTechAsia stands for," adds Mr Wong. "Continuing the 40 year legacy of CommunicAsia and BroadcastAsia, the new ConnecTechAsia will continue to serve Asia as we embark on the journey of the Fourth Industrial Revolution." SST

IFSEC International 2018
19-21 June 2018
ExCeL London UK

DISCOVER THE LATEST IN SECURITY TECH AT IFSEC INTERNATIONAL 2018

IFSEC international 2018 will be held in London this year at an opportune time when security tech isn developing at a rapid pace thanks to the advent of the internet of things, robotics and artificial intelligence. IFSEC 2018 has always been known to be the world's centralised gateway to the critical security conversation. Amidst mutating threats, the integrated path to achieving global safety starts with IFSEC 2018.

The event spanning 3 days will afford visitors the opportunity to Access inspiring high-level panel debates from government and industry influencers, and join the collaborative conversation between installer, integrator, end user and vendor as well as explore the high-quality solutions they need while addressing their security issues with the experts behind every innovation they hope to procure. Visitors will also be able to decide on impartial verdicts for security solutions against rigorous, real life testing zones, including attack scenarios and surveillance and research the inspiring ways you can adapt to the changing tides of tomorrow's security challenges and equip yourself with the tools you need to move forward with certainty. Then of course there is the opportunity to network with the global security industry whilst sophisticated partnerships and inspiring collaborations kickstart under the same roof.

The show will feature interesting highlights this year that are all encompassing of the latest and greatest in security tech with regards to the latest innovations on the market.

Borders and Infrastructure

The borders and infrastructure exhibition will focus on border security. On exhibition will be products, solutions and learning for large scale security issues as faced by industries such as border control, critical national infrastructure, transport, healthcare and key strategic assets.

Future of Security Seminar Theatre

Attendees can also look forward to security industry insights and prospects with this interesting seminar that will cover a range of essential CPD accredited presentations on the very latest in security technology design and integration.

Attack Zone

Attendees can expect a hands-on experience at the show in the Attack Zone where they will be able to watch expert technicians

"The exhibitor list features companies from all over the world including but not limited to Hungary, The United Kingdom, South Korea, Hong Kong, China, Italy, the United States and France. Categories include fire safety, access control, cyber security, integrated security, perimeter protection, video surveillance and many more."

from LPCB/BRE put perimeter solutions to the test in a series of real-life attacks, live on the IFSEC show floor and witness LPCB accredited fencing, shutters, doors and covers tested against non-certified alternatives and see how they fair.
Drone Zone

Perhaps one of the most exciting zones will be the drone zone featuring the latest players in the security industry that has everyone talking these days. Drones are able to monitor and secure places that human security guards are unable to which is why they are the talk of the town these days with the big companies such as Dahua getting in on the action. Whether one is looking to use drones as part of their current security strategy, or looking to protect their business against them, they will be able to get up close and personal to the action in this zone.

Engineers of Tomorrow

At this zone, attendees will be able to Promote their businesses young talent, aid their learning, showcase their organisation, and highlight their commitment to employee development.

All in all, the show will feature over 350 exhibitors from different aspects of the security industry both physical and cyber security. Some of the names include well known names such as FLIR Systems, Inc. , the leading developer of open-standard, end-to-end video surveillance solutions, including integrated video management systems (VMS), thermal imaging cameras, motorized IP cameras and advanced video analytics and Logipix Technical Development that provides high quality IP based video solutions for traffic and city surveillance and critical infrastructure protection market.

The exhibitor list features companies from all over the world including but not limited to Hungary, The United Kingdom, South Korea, Hong Kong, China, Italy, the United States and France. Categories include fire safety, access control, cyber security, integrated security, perimeter protection, video surveillance and many more.

The visitors of the event comprise of a diverse range of security industry professionals such as heads of both physical and cyber security, global security directors, strategy directors, general managers and much more. There will also be global technical advisors and distributors present.

For more information, please visit: www.ifsec.events/international

Subscription Form

Fax your order today
+65 6842 2581

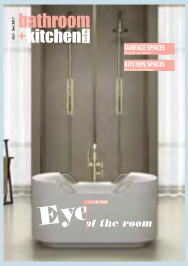
(Please tick in the boxes)

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

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: ______________

IoT Asia 2018
21 – 22 March 2018
Singapore Expo

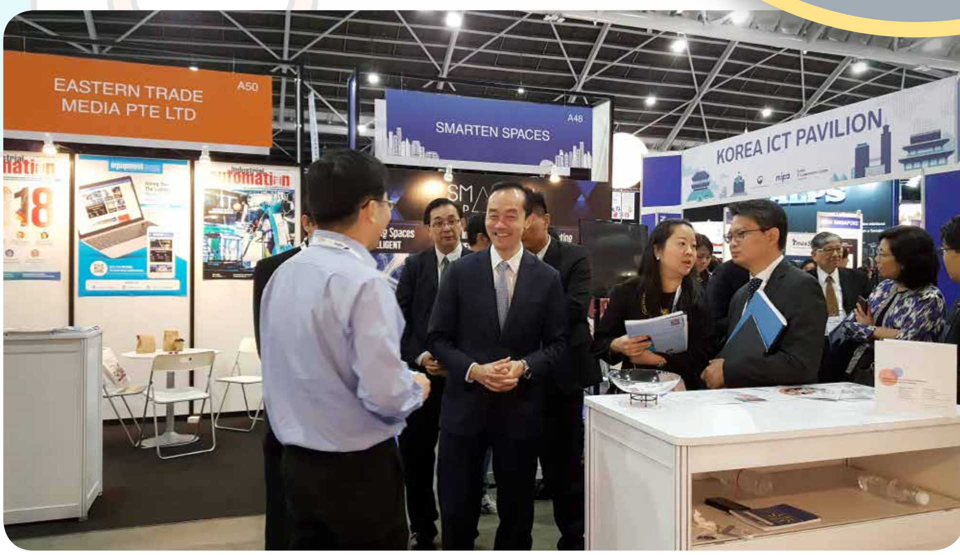
EXPLORING DIGITALISATION AND CONNECTIVITY AT IOT ASIA 2018!

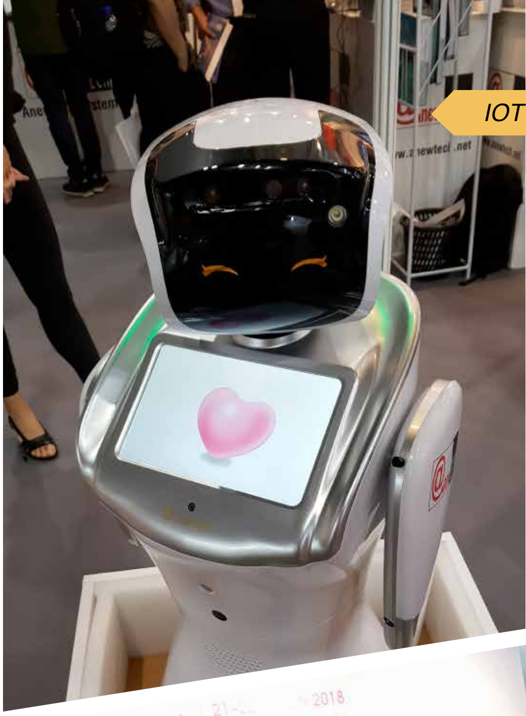
Highlights from one of 2018's most innovative shows

IoT Asia 2018 was held for the second time this year at Singapore Expo. In a time where the concept of connectivity is becoming commonplace and digitalisation across various sectors is becoming a necessity, this show has proven to be an excellent platform for showcasing the latest and more importantly, the SMARTEST technology that is available in the industry for building automation as well as security. In the Global Smart City Performance Index survey conducted by Intel, Singapore currently ranks as the number 1 SMART City in the world due to the usage of IoT-enabled infrastructure in public transportation as well other areas. The island nation is therefore the perfect venue for innovators, the government and academics to convene and explore the science of connected technology.

The Guest of Honour for this year was Minister-in-charge of the Smart Nation initiative Dr Vivian Balakrishnan who delivered his thought provoking speech at the opening ceremony welcoming visitors and delegates like. He expressed that there is a need for open standards and for vendors to adapt their products to these standards. "It is the Government's duty to provide the necessary infrastructure so that vendors in the private sector can design their products and services to fit into the open standards and the Government's systems", he said. With regards to the vulnerabilities of connected products and solutions, he added that vendors must ensure that security "is baked into" their products and services and it should not be a case of a "belated scramble" to tackle such issues after the product or service is rolled out.

The lineup of innovative products and solutions featured at IoT Asia this year





included autonomous security robots, drones capable of ariel monitoring, IP cameras with biometric features and even an interactive CCTV camera complete with animated eyes for that cute effect. On disply were also cyber security solutions to hack proof facilities and property alike which only reinforced the fact that all companies are currently confronting the possibility of compromised safety when their IoT devices are not secure. There were about 139 exhibitors this year from countries such as France, Taiwan, Japan, Korea along with Singapore that consisted of industryleaders such as TATA Communications, Avenet, SigFox and Singtel as well as various startups. Attendees were also treated to never before seen products such as the cute but efficient robot from Anewtech Systems that wandered the premises greeting visitors and delegates alike with its endearing eyes and intriguing features. In the Taiwanese pavillion, visitors were offered the opportunity to view a lineup of drones and other ground breaking aeriel monitoring technology presented by companies such as Amaryllo International and Coretronic. There were also a multitude of startups displaying the latest developments in cyber security and data analytics.

Other than the exhibition, IoT Asia 2018 also featured several conferences throughout the 2-day period focusing on SMART cities as well as Industrial IoT. These conferences focused on topics such as the ability of the IoT to transform businesses, concepts such as cashless payments and the global digital economy and how digitalisation and IoT influences government policies and vise versa. The second day's conferences were dedicated to industrial IoT and touched on subjects such as

> *"Vendors must ensure that security 'is baked into' their products and services and it should not be a case of a 'belated scramble' to tackle such issues after the product or service is rolled out."*

the state of the industry currently and how it is transforming itself in relation to digitalisation and the internet of everything. There was also a focus on cyber security, specifically on quantum computing, its significance for industrial applications and opportunities for solving extant problems in security encryption, data privacy and trust with quantum innovations. The conferences concluded on a thought-provoking note as panellists from all over the world discussed the implications of industry digitalisation and transformation in Asia and how it would in both the public and private sector.

All in all, IoT Asia turned out to be a truly diverse and multifaceted shpw in terms of displaying to the world the innovations that Asia has to offer as the current leader in the area of SMART cities and the internet of everything. SST

ADVERTISERS' INDEX

BMAM EXPO ASIA 2018	15	IFSEC PHILIPPINES 2018	3
CHINA SECURITY 2018	11	IFSEC SOUTHEAST ASIA 2018	1
COUNTER TERROR ASIA EXPO 2018	5	MICROENGINE TECHNOLOGY	7
DELTA SCIENTIFIC	9	SAFETY & SECURITY ASIA 2018	IBC
GUANGZHOU PUBLIC SECURITY TECHNOLOGY 2018	13	ZHEJIANG DAHUA	IFC
IFSEC INTERNATIONAL	OBC		