Security Solutions Today

July / August 2019

TECHNOLOGY IS RESHAPING MUSEUM & BORDER SECURITY

In Focus
What Every Security Leader Needs to Know

In Focus
A Great Leap Forward In Human-Machine Interface?

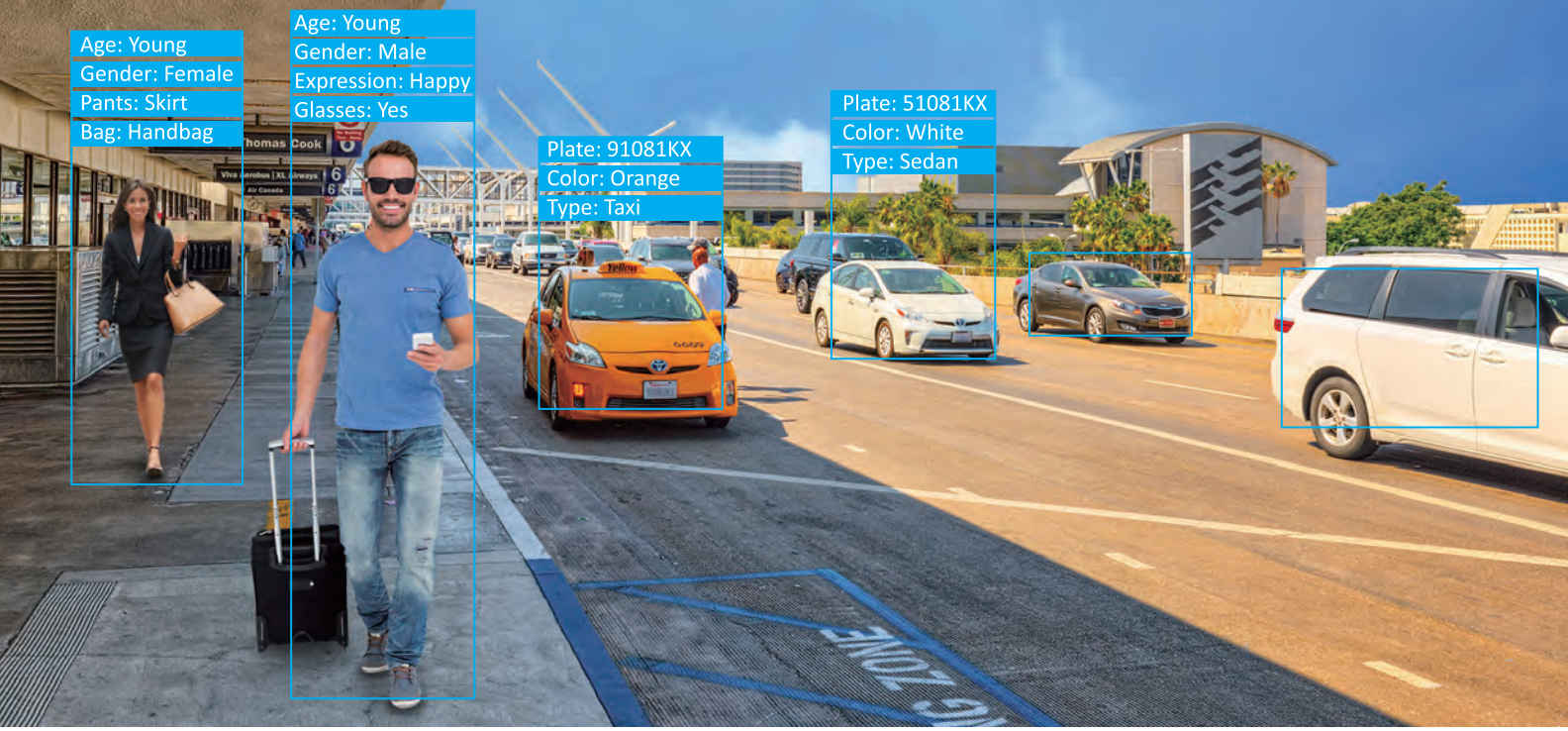
Inside Look
One Million CCTVs In London By 2025

Inside Look
From Fortress To Airport Mode

Scan this to download the latest issue from our website

IVSS2.0-Gear Up For AI

Robust AI computing empowers rich applications



- **Scalable GPU:** Design to meet the ever-growing project requirements.
- **Face recognition:** Real-time crosscheck to find out the face by target features with high accuracy.
- **Perimeter protection:** Focus on human/vehicle and filter out false alarms caused by animals, rustling leaves, bright lights, etc.
- **Video metadata:** Quick search by metadata of human face/human body/motor vehicle/non-motor vehicle.
- **Intuitive Interface:** Unified GUI for local and remote application offers excellent user experience and unique PC client can avoid issues from browser and plug-in.

Recommended Models

IVSS7008-1I
IVSS7008-2I

IVSS7016 (DR)-4I
IVSS7016 (DR)-8I

IVSS7024 (DR)-8I
IVSS7024 (DR)-16I

ISO 9001:2000

DAHUA TECHNOLOGY SINGAPORE PTE. LTD.
Add: 62 Ubi Road 1#06-15 Oxley Biz Hub 2 Singapore 408734
Tel: 65 6538 0952
Email: sales.sg@dahuatech.com
Facebook: @DahuaTechnologySpore

Safety & Security Asia 2019

The 18TH International Safety & Security Technology & Equipment Exhibition

1 - 3 October 2019

Halls B & C, Marina Bay Sands, Singapore

10,000sqm gross exhibition space • **250 exhibitors** from 20 countries • **9,000 trade professionals** from 40 countries

*Combined statistics across Architecture & Building Services 2019

Be a part of **Safety & Security Asia 2019** - the quality sourcing platform for excellent commercial security solutions. Showcase your latest technologies, innovations and related services in the safety and security arena in the most established and longest-running commercial security tradeshow in ASEAN!

JOIN SSA 2019 TODAY AND

Expand your business network and explore new opportunities
Stay updated on industry trends and developments
Maximise your marketing & publicity efforts

For booth enquiries, contact:
SSA@cems.com.sg or call
(65) 6278 8666
www.safetysecurityasia.com.sg

A Part Of
Architecture & Building Services 2019
Providing Solutions for Smart Nation Building

Organised By CEMS
Conference & Exhibition Management Services Pte, Ltd.

1 Maritime Square #09-43, HarbourFront Centre, Singapore 099253
info@cems.com.sg • (65) 6278 8666

IN THIS ISSUE

The Most Satisfying Phrase Heard after a Vehicle Attack...

"Defended by **DELTA**"

For advanced vehicle access control systems that stop terrorists dead, contact the company that started the industry. Worldwide security specialists depend upon Delta Scientific for crash-rated systems that include surface mounted and high security barricades, bollards, beams, portable barriers, sliding gates, guard booths and parking control systems. You can see our full product line by visiting our website at **www.deltascientific.com**. Get *"Defended by Delta"* today.

*You asked for it; we made it! The lighter weight, DC-operated, K4 certified Delta **DSC1500** portable beam barricade is available for purchase today.*

DELTA

Visit **www.deltascientific.com** for details and specifications.
GSA 47QSWA18D003B ▲ **1-661-575-1100** ▲ **info@deltascientific.com**

CONTACT

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

EDITOR
Michelle Lee
(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)

PLATINUM PARTNER
Security Solutions Today

alhua TECHNOLOGY

Images/Vectors Credit: Freepik.com

Designed by Siti Nur Aishah

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
MCI (P) 084/05/2019 | ISSN 2345-7104 (Print)

Printed in Singapore by
Refine Printing Pte Ltd (L011/06/2019)

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 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

ISSN 2345-7104

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

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

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

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

MicroEngine®

Integrated Security Systems

The Trusted Brand in Security Solutions

NO CLOUD
NO SUBSCRIPTION

OnPremQR™

Mobile Identification System

- Innovative QR Code based security system
- On Premise mode, no Cloud subscription
- Better option for Non Cloud-Ready Offices
- Clone detection with Dynamic QR Code
- Higher security using AES128 Encryption
- Works with our Integrated Security System

Plato QR Code Reader

Available on the iPhone App Store

ANDROID APP ON Google play

1300-88-3925 or enquiry@microengine.net

www.microengine.net

DESIGNED BY MALAYSIAN
MADE IN MALAYSIA

REG No. 749921389

COMING SOON...

AUGUST

Secutech Vietnam 2019

Date: 14 - 16 August 2019
Venue: Ho Chi Minh City, Vietnam
Telephone: +886 2 8729 1099 ext. 768
Website: www.secutechvietnam.com
Email: michelle.chu@newera.messefrankfurt.com

SEPTEMBER

Smart Cities & Buildings Asia 2019 / IBEW 2019

Date: 4 - 6 September 2019
Venue: Sands Expo & Convention Centre, Marina Bay Sands, Singapore
Telephone: +65 6780 4594
Website: www.scb-asia.com
Email: info@scb-asia.com

SEPTEMBER

GSX 2019

Date: 8-12 September 2019
Venue: Mccormick Place, Chicago, IL
Telephone: +1.888.887.8072, +1 972.349.7452
Website: www.gsx.org
Email: asis@asisonline.org

OCTOBER

Safety & Security Asia 2019

Date: 1 - 3 October 2019
Venue: Marina Bay Sands, Singapore
Telephone: +65 6278 8666
Website: www.safetysecurityasia.com.sg
Email: SSA@cems.com.sg

OCTOBER

Secutech Thailand 2019

Date: 28 - 31 October 2019
Venue: Bangkok, Thailand
Telephone: +886 2 8729 1099 ext. 215
Website: www.secutechthailand.com
Email: jason.cheng@newera.messefrankfurt.com

JUNE 2020

IFSEC SEA 2020

Date: 23 - 25 Jun 2020
Venue: Malaysia International Trade and Exhibition Centre, Kuala Lumpur, Malaysia
Telephone: +60 3-9771 2688
Website: www.ifsec.events/kl/
Email: ifseccustomerservice@ubm.com

MAY 2020

IFSEC International 2020

Date: 19 - 21 May 2020
Venue: ExCeL, London, UK
Telephone: +65 6780 4594
Website: www.ifsec.events/international/
Email: ifseccustomerservice@ubm.com

JULY 2020

IFSEC Philippines 2020

Date: 22 - 24 July 2020
Venue: SMX Convention Center, Pasay City, Metro Manila, Philippines
Telephone: +63 2 581 1918
Website: www.ifsec.events/philippines/
Email: ifseccustomerservice@ubm.com

IBEW
INTERNATIONAL BUILT ENVIRONMENT WEEK

3 – 6 SEPTEMBER 2019
MARINA BAY SANDS, SINGAPORE

Expect a whole new experience with IBEW 2019!

4 ANCHOR EXHIBITIONS UNDER IBEW

New all-in-one platform that combines sustainability, productivity, energy efficiency as well as smart city solutions and innovations. Together, the 4 tradeshows will gather over 550 exhibiting brands and 9 pavilions from across the region with 12,000 industry professionals expected to convene at IBEW 2019.

SUSTAINABILITY — BEX ASIA

ENERGY EFFICIENCY — mce ASIA mostra convegno expocomfort

PRODUCTIVITY — INNO BUILD ASIA

SMART TECHNOLOGIES — SMART CITIES & BUILDINGS ASIA

For exhibitions, contact

T: +65 6780 4658

E: Gladys.heng@reedexpo.com.sg w: www.builtenvironment.com.sg

IBEC 2019 SPEAKERS

Gain insights from over 80 expert speakers as they share their knowledge and experience in environmental sustainability, construction productivity and smart facilities management.

Dr. Ayesha Khanna
CEO
ADDO AI

Mr. Cheng Hsing Yao
Group Managing Director
Guocoland (Singapore)
Pte Ltd

Dr. Chris Luebkeman
Arup Fellow Director of
Global Foresight, Research
+ Innovation

Ms. Lisa Bate
Chair
World GBC

For conference, contact

T: +65 6780 4658

E: wingyan.lam@reedexpo.com.sg w: www.ibew.sg

Register before 31 July
to enjoy early bird rate!

IBEW Organiser
Building and Construction Authority

Exhibitions Organiser
Reed Exhibitions

An Event of
IBEW

EDITOR'S NOTE

Dear esteemed reader,

The security challenges for museums are complex. Museums must protect priceless art pieces against vandalism, theft and damage while allowing millions of people access to the cultural treasures they house each year.

So what makes a museum secure? In this issue, we showcase the security behind El Museo Thyssen-Bornemisza in Madrid, home to some of the world's finest pieces of art.

This issue we also look at how border agencies are increasingly embracing emerging technologies. In June, Canada and The Netherlands shook hands on paperless border clearance between the two countries. Travellers flying between the two countries need only a simple face scan to board a plane and to clear immigration on arrival.

Above all, this issue is about change. Miju Han, Director of Product Management at HackerOne, articulates how businesses must change from their traditional cybersecurity 'fortress' strategy to behaving more like an airport. Meanwhile Ken Lim of Johnson Controls explains why organisations must change the way they protect their smart buildings.

Happy reading!

Michelle Lee

Editor

secutech THAILAND

Concurrent with

fire & safety powered by Secutech Thailand

SMART Living powered by Secutech Thailand

info security powered by Secutech Thailand

smart city solution powered by Secutech Thailand

28 – 31 October 2019 • Bangkok, Thailand • www.secutechthailand.com

In collaboration with:
Digital Economy Promotion Agency depa

The largest security, fire and smart living & home and info security fair in Thailand reflects the growing smart city developments

Increase of smart cities can be seen across the country as Thailand 4.0 set its mark with development of various infrastructure projects with high investments across all verticals in the Eastern Economic Corridor (EEC). Secutech Thailand will be returning as the center for answering the demand of security, fire safety and smart living & home and info security technologies in smart cities.

2019 Show features

- 250+ Exhibitors
- 7,500+ sqm
- VIP 16+ Exclusive VIP tours

Top vertical projects in the EEC

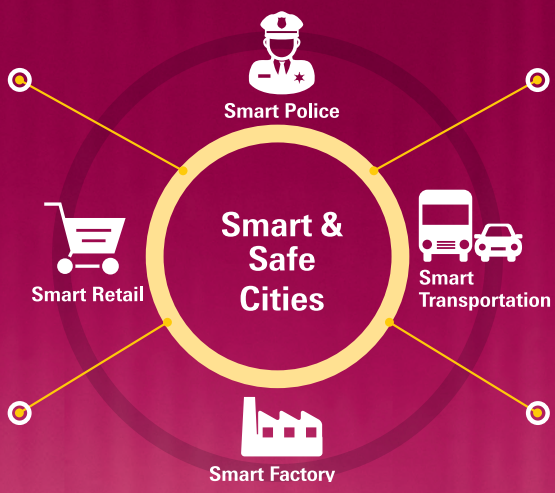
- International airports
- High-speed rails
- Motorways
- Sea ports
- Hospitals
- Tourism
- Industrial factories

INTELLIGENT SECURITY

- Intelligent video & AI-enhanced surveillance
- Biometric identification
- Smart sensors & alarm
- Gate control

FIRE & SAFETY

- Active fire protection
- Passive fire protection
- Disaster prevention
- Efficient rescue
- Personal protection



SMART LIVING

- Intelligent homes
- Residential security & safety
- Elderly & home care

SMART CITY SOLUTION

- Environmental management
- Waste management
- Water management

INFO SECURITY

- IoT security
- Mobile security
- Cloud security
- Network & endpoint security
- Risk remediation

messe frankfurt

WORLDEX Group of Exhibition Companies

Organiser contact

Messe Frankfurt New Era Business Media Ltd
Jason Cheng I +886 2 8729 1099 ext. 215
jason.cheng@newera.messefrankfurt.com

Lowering The Total Cost Of Ownership Of Video Surveillance With An Umbrella

Qognify has launched a web-based system that reduces operational costs and simplifies the management of large-scale distributed surveillance camera networks.

Umbrella delivers significant cost savings by managing large distributed video surveillance systems centrally in the cloud. The management solution is fully integrated with Qognify's video management software (VMS) Cayuga.

In recent years, video surveillance projects have become larger and more complex, demanding more resources and increasing operational costs. Altering the configuration of multiple sites is time-consuming and monitoring the health status of all servers and cameras across every location is a challenge. As a consequence, organisations frequently overspend on technical expertise and unnecessary licenses, as well as potentially expose themselves to regulatory risk.

The technology solution provider for physical security and enterprise incident management solved these challenges by launching the web-based Umbrella, which can be hosted in the cloud (including Microsoft Azure and AWS) as well as on premises.

Once installed, Umbrella provides a consolidated view of all servers and cameras across every connected installation, highlighting those that require attention. Furthermore, if any company-wide changes are required to be made to how the video system operates (for example due to changes in regulations), they can be configured and rolled out remotely and immediately.

Umbrella is suited for organisations in the banking, retail, logistics and transportation industries, which operate large-scale branch networks with hundreds of sites and thousands of cameras. These organisations also place a premium on their physical security strategy.

Said Steve Shine, CEO of Qognify, "Launching Umbrella, we want to fundamentally change the way organisations deploy, use and manage technology to protect people, customers, assets and infrastructure." SST

All New HP Laptops Will Have Deep Instinct's Malware Protection Preinstalled

HP Inc. is installing malware protection software by Israeli startup Deep Instinct Inc. on all its new lines of laptops.

HP Sure Sense, Deep Instinct's deep learning-based predictive threat prevention software, will be preinstalled on HP's latest EliteBook and HP ZBook devices. With more than 350,000 new, increasingly complex malware varieties being discovered daily, HP required a new line of cybersecurity defence powerful enough to protect customers against rapidly evolving threats without affecting system performance.

Through the power of autonomous AI and deep learning, HP Sure Sense quickly combats progressively sophisticated cyber threats without requiring an army of security experts.

By leveraging Deep Instinct's deep learning-based threat prevention engine, HP Sure Sense provides real-time detection and prevention coupled with anti-ransomware behavioural protection. With its high detection rates of known and unknown malware (>99.9 percent), and low false positive rate, HP Sure Sense is capable of scanning any file type while predicting and preventing known and unknown threats before damage occurs.

SE Labs' independent threat prevention evaluation test labs report showed that Deep Instinct achieved a 100% prevention rate and zero false-positives when detecting and blocking known and unknown threats, including file-based and file-less attacks.

HP Sure Sense is a standalone, self-managed solution that works on or offline, offering simple, streamlined user experience. It enables real-time cyber protection across all endpoints, servers, mobile devices and operating systems.

"By teaming up with Deep Instinct on the development of HP Sure Sense, we are providing end users with a powerful solution that confidently predicts and prevents security threats both today and in the future," said Andy Rhodes, Global Head Commercial Personal Systems for HP Inc.

Founded in 2015, Deep Instinct has raised $64 million to date from investors like Nvidia Corporation and has offices in Tel Aviv and New York. Deep Instinct's customers include Air Asia as well as governments. SST

secutech VIETNAM

Concurrent with

fire & safety powered by Secutech Vietnam

SM building powered by Secutech Vietnam

14 – 16 August 2019 • Ho Chi Minh City, Vietnam • www.secutechvietnam.com

Featuring official supporters
- APSA Vietnam
- Department of Fire Prevention & Rescue
- Directorate for Roads of Vietnam
- Vietnam Railway Authority

Profit from Vietnam's strong fundamentals and robust building demands at the leading security, fire safety and smart building hub

As one of the fastest-growing markets among ASEAN countries, Vietnam is home to a surging amount of business opportunities with large demands for security, IoT and fire safety systems and solutions.

2019 Show features

360+ Exhibitors

11,000+ sqm

20+ Seminar sessions

Top vertical projects in Vietnam

Industrial
• Factories • Technology parks • Power plants

Transportation
• Railways • Highways • City transportation
★ **New supporters:** Directorate for Roads of Vietnam, Vietnam Railway Authority

Hospitality
• Hotels • Service apartments • Villas

Commercial
• Shopping malls • High-rise buildings
• Offices • Retail

Residential
• Residential communities • Single houses
• Mix-used residential buildings

5 Reasons not to miss Secutech Vietnam

Organiser contact

Messe Frankfurt New Era Business Media Ltd
Michelle Chu I +886 2 8729 1099 ext. 768
michelle.chu@newera.messefrankfurt.com

messe frankfurt

VIETFAIR

ArmorMe Backpack With Bulletproof Panel For Student Safety

It looks and feels like a regular canvas backpack but the ArmorMe brand of bulletproof backpacks is reinforced with a bullet-resistant material that can help protect students in the event of a violent shooting incident.

Developed by Israeli security experts, the backpack is made with solid level IIIA NIJ Protective Panels, the super-strong bulletproof material used in personal armour including combat helmets and bulletproof vests.

Field tested by Israeli security and military experts, the backpack features an easy-on, easy-off design for speedy engagement.

The ArmorMe backpack was developed amidst the reality of increasing deadly violence in school campuses. Since the Sandy Hook Elementary School shooting in 2012, there have been more than 2,000 mass shootings in the US. Nearly 2,300 people have been killed and almost 8,400 wounded. In 2018 alone there have been 97 school shootings and almost 200,000 students in the United States have been exposed to shooting on campus during school hours.

"These grim statistics are an unfortunate fact of life in the United States. School shootings are happening and, more importantly, they are getting deadlier," said security specialist and Israel Defense Forces Colonel (ret). Gabi Siboni.

"We built this backpack to address the daily reality of student life. We wanted a pack that is stylish, light and comfortable, could carry a laptop and that would last multiple academic years. At the same time, we built this backpack to withstand gunshots."

A single paneled backpack costs $160 to $190 with coverage from neck to knee when worn in front. The double-paneled backpack costs $210 to $250 and provides coverage for both sides of the torso. The bags are available at Amazon and at ArmorMe.com. SST






IFSEC INTERNATIONAL

informa markets

SAVE THE DATE

IFSEC International returns

19-21 May 2020, ExCeL London

Co-located with:

FIREX INTERNATIONAL

SAFETY & HEALTH EXPO

FACILITIES SHOW

Plus:

CTX COUNTER TERROR EXPO 19-21 May 2020 ExCeL, London

FORENSICS EUROPE EXPO 19-21 May 2020 ExCeL, London

AMBITION THE EPRR EXPO 19-21 May 2020 ExCeL, London

Check Point Research Launches Repository For Vulnerabilities

Check Point Research, the threat intelligence arm of Check Point Software Technologies Ltd., a leading provider of cyber security solutions globally, has launched a new online vulnerability repository, CPR-Zero.

Check Point will publicly list all vulnerabilities its research team finds on CPR-Zero. The move makes Check Point the industry's largest cyber security vendor to openly share such information.

CPR Zero was launched with over 130 vulnerabilities and will quickly expand to offer a comprehensive library of all vulnerabilities that Check Point's research team has uncovered, both historic and in the future. The repository will be continually updated with new discoveries.

The vulnerabilities are indexed and easily accessible. CPR Zero lists Common Vulnerabilities and Exposures (CVEs) with links and references for viewers to learn more from the official CVE database. The list also contains detailed information regarding each vulnerability, including a crash and dump and a short explanation.

"Check Point's mission is to make the online world a safer place to live in. To help us further get there, we are making the bold move to be the largest cybersecurity company in the industry to share all our technical CVE findings with everyone," said Neatsun Ziv, VP of Threat Prevention. "No other cybersecurity company of our size has taken this step."

CPR Zero is Check Point's latest initiative in responsibly notifying both consumers and enterprise organisations of new cybersecurity risks.

The website for CPR Zero is cpr-zero.checkpoint.com SST

Next-Generation Drone-In-A-Box Launched

Percepto, a drone solutions company, has launched the next generation of its AI-powered autonomous industrial Drone-in-a-Box. Drone in a box is an emerging autonomous technology. Unlike traditional drones (also known as unmanned aerial vehicles), which consists of both a non-manned aircraft and some form of ground-based controller, the drone in a box autonomously deploys from and returns to self-contained landing 'boxes'. The box functions as a landing pad and charging base. After carrying out a pre-programmed list of instructions, the drone in a box returns to its base to charge or upload information.

Available now, the Percepto solution includes a highly portable, smaller, lighter weight and extreme weather-resistant base station. Adding field-proven 5G compatibility, the new Drone-in-a-Box also features seamless integration of 2D mapping

and 3D modelling, highly customised reporting, comprehensive compliance and enhanced safety functions. In the event of loss of GPS, the solution is able to accurately log the drone's position.

The solution provides constant aerial visual insights. It enables companies in mining, energy and industrial, oil and gas, ports and terminals sectors to optimise their security and business operations, while reducing risks and operational costs.

Smaller, Lighter Weight, Weather-resistant And Highly Portable

At only 166(W) x 162(D) x 168(H) and weighing 162kg, the smaller and lighter weight Percepto Base makes it even easier to transport, deploy and manoeuvre into position.

The new Percepto Base achieves an ingress protection rating of IP65, which promises complete protection against contact with moving parts inside the enclosure and against the ingress of dust.

Highly Customisable Reports

Powered by the Percepto Core Software suite, the solution delivers highly customised reports, allowing companies to translate aerial data from Sparrow drones to actionable insights. Each stakeholder operating onsite received aerial insights relevant to its field of interest. SST

Part of the
ASEAN Super 8 Series

IFSEC SOUTHEAST ASIA

SECURITY • FIRE • SAFETY

23 - 25 JUNE 2020

MALAYSIA INTERNATIONAL TRADE AND EXHIBITION CENTRE (MITEC), KL

SECURITY IS CRITICAL
IFSEC IS ESSENTIAL

Organised By
informa markets | UBM

WWW.IFSECSEA.COM

@IFSECSEA #IFSECSEA IFSEC Southeast Asia

Dallmeier Integrates AnyVision Facial Recognition Into Its Software Platform For Security

German manufacturer Dallmeier is integrating AnyVision's facial recognition technology into the Dallmeier HEMISPHERE.

Dallmeier manufactures solutions for security applications and process optimisation including cameras, recording systems and software. Its solutions are used worldwide in safe cities, stadiums, airports, logistics, casinos and the processing industry.

A pioneer in AI-based facial, body and object recognition, AnyVision currently develops technology for security and surveillance, mobile authentication, access control and real-world analytics. AnyVision's software is plug-and-play for new and existing systems, and able to overcome challenges such as occlusions, different angles of views and poor lighting conditions.

The HEMISPHERE software platform offers industry clients modular solutions for security applications and business process optimisation.

From the optimisation of marketing activities to forensic evaluations, the use of facial recognition technologies is becoming increasingly important for customers of video technology solutions. The integration of AnyVision's technology will enable Dallmeier customers to utilise facial recognition data within the various modules of the Dallmeier HEMISPHERE software platform.

With this, security and business processes can be optimised, for example, by enabling blacklist/whitelist procedures, marketing optimisation through VIP-customer recognition, forensic evaluations in law enforcement procedures and the automation of access control in office or manufacturing environments.

"In today's increasingly complex world, customers need solutions that can integrate powerful components from leading manufacturers within a single platform strategy. Partnerships like this with AnyVision ensure that our customers always have the optimal combination of leading technologies at their disposal," said Dieter Dallmeier, Founder & CEO, Dallmeier. SST

Launch of Spoof-Proof Fingerprint Scanner

Suprema ID has launched a fingerprint scanner that the global provider of biometrics and ID solutions claims is spoof-proof.

Featuring Suprema's latest deep-learning based LFD (live fingerprint detection) technology, the new BioMini Slim 3 effectively prevents spoofing with fake fingerprints using various materials including rubber, silicon, film and paper.

The new FAP30-compliant scanner comes with the world's slimmest optical sensor. With the FAP30-compliant wider platen, the scanner now captures a wider area of fingerprints for more accurate reading. The sensor's slim form factor also allows for extra flexibility in design when loaded in mobile devices. In addition, BioMini Slim 3 also features Multi-Dynamic-Range technology that enables users to capture high quality fingerprints under harsh environments and under direct sunlight of up to 100,000 LUX. SST

IFSEC PHILIPPINES

SECURITY • FIRE • SAFETY

22 – 24 JULY 2020

SMX CONVENTION CENTER
PASAY CITY, METRO MANILA

THE LEADING **SECURITY, FIRE** AND **SAFETY** EVENT IN PHILIPPINES

Organised By
informa markets | UBM

WWW.IFSECPHILIPPINES.COM

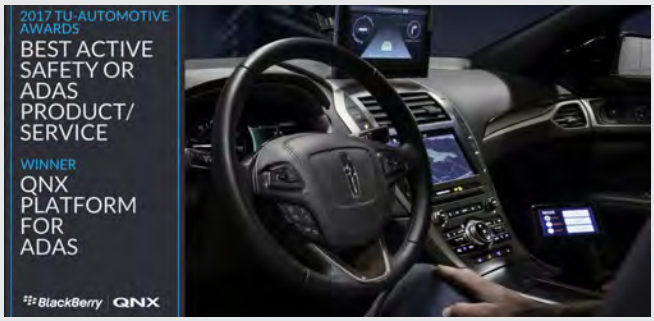
@IFSECPH #IFSECPHILIPPINES IFSECPHILIPPINES

BlackBerry's QNX Software Now Embedded In More Than 150 Million Vehicles

BlackBerry's QNX software is now embedded in more than 150 million cars on the road today. This is an increase of 30 million cars since the leader in automotive cybersecurity reported its automotive footprint in 2018.

BlackBerry has the highest level of automotive certification for functional safety with ISO 26262 ASIL D and decades of experience in powering mission-critical embedded systems in automotive and other industries. The QNX Platform for ADAS was recognised at the 2017 TU-Automotive Awards as the Best Active Safety or ADAS Product/Service.

Automotive OEMs and tier ones use BlackBerry QNX technology in their advanced driver assistance systems, digital instrument clusters, connectivity modules, handsfree systems and infotainment systems that appear in car brands such as Audi, BMW, Ford, GM, Honda, Hyundai, Jaguar Land Rover, KIA, Maserati, Mercedes-Benz, Porsche, Toyota and Volkswagen.



BlackBerry QNX technology includes QNX Neutrino OS, QNX Platform for ADAS, QNX OS for Safety, QNX CAR Platform for Infotainment, QNX Platform for Digital Cockpits, QNX Hypervisor 2.0 and QNX acoustics middleware. SST

Plug-And-Play 3D Face Recognition Solutions For Smart Consumer And Commercial Devices

ams, a leading worldwide supplier of high performance sensor solutions, and artificial intelligence pioneer MEGVII are collaborating to jointly develop plug-and-play 3D face recognition solutions for any type of smart consumer and commercial device. They plan to bring their joint solution to market before the end of 2019.

The two companies will offer the world's first off-the-shelf face recognition system for smart home, smart retail, smart building and smart security applications, completely independent of the user's mobile phone.

Consumers Prefer Face Recognition For ID Authentication

Mobile phone users have rapidly adopted face recognition as their preferred means of user authentication, especially for security reasons. Manufacturers of other types of products are now keen to gain the convenience and security benefits of implementing face recognition.

The integrated solution under development combines ams' proven Vertical-Cavity Surface-Emitting Laser emitter modules with MEGVII's software for depth mapping and face recognition. This will yield the first 3D Active Stereo solution with robust performance under both indoor and outdoor light conditions. In addition, the solution is expected to meet high security standards making it suitable for use in consumer payments systems such as point-of-sale terminals.

Previously MEGVII and ams have cooperated successfully to develop a complete face recognition solution for mobile phones. The new solution however will be compatible with a much wider range of applications processors from various manufacturers. This will greatly reduce the development time, risk and effort involved in implementing face recognition in embedded systems such as smart locks, access control equipment and payment terminals. SST

GSX
GLOBAL SECURITY EXCHANGE

FORMERLY ASIS ANNUAL SEMINAR & EXHIBITS

8-12 SEPTEMBER 2019
McCORMICK PLACE | CHICAGO, IL

GSX.ORG | #GSX19

A Smarter EXCHANGE

GSX provides an invaluable opportunity to explore countless topics ranging from AI to VR, IoT security to insider threats, and robotics to radicalization—each delivering valuable, actionable takeaways to help shape your strategy—today and in the future.

20,000 registered attendees

110+ countries

300+ education sessions

Up to **30 CPEs**

2 X learning theaters in the Exhibit Hall

1 Global Exchange

See full education lineup by reviewing our conference brochure or go to
GSX.org/SST

New Altronix Switch Supports Up To Four IP Access Controllers In A Single Enclosure

Altronix, a provider of power and data transmission solutions for the professional security industry, continues to expand its line of networking products with the release of the new NetWay5B 5-Port Hardened Switch.

This compact IP switch is designed to mount in virtually any Altronix enclosure and easily combines multiple IP devices over a single Ethernet cable–back to the head-end. It is especially suitable in the Trove series where multiple IP access controllers from the industry's leading manufacturers are deployed.

NetWay5B greatly reduces installation costs by eliminating the need and costs associated with running dedicated cables for each deployed device. It features five 10/100/1000 data ports with speed/activity LED indicators, and is powered via PoE or any 12 or 24VDC UL listed power source. As with all Altronix products, the new NetWay5B is manufactured in the U.S.A., and backed by a lifetime warranty.

Also available is the BR1 Mounting Bracket, which allows for additional Altronix sub-assemblies to be mounted to the enclosure's side wall. This add-on mounting bracket, compatible with Trove and Maximal series enclosures, makes it even easier for system expansion. SST

Laser-Powered Sensor To Kick Off 'Anonymised' Security Era

A sensor that uses an array of lasers to detect objects, people and vehicles could herald an era of anonymised surveillance that isolates threats from uninvolved people or objects.

Cepton Technologies has released Vista-Edge Perception Evaluation Kit (PEK), an edge processing system that combines Cepton's Vista LiDAR sensor and the NVIDIA Jetson TX2 supercomputer on a module. The technology made its debut at IFSEC International in London.

PEK possesses the unerring accuracy of lasers to scan the environment in much the same way a radar does, but at a much higher resolution, building an image of the world around it regardless of lighting conditions.

It offers other advantages over traditional sensors. It can see in the dark and it only transmits a fraction of the information a video would, reducing the burden of data storage and network bandwidth charges, while opening the door to more mobile installations. It is a plug and play device. Out of the box, the system takes only a few minutes to set up.

PEK comes pre-installed with Cepton's object tracking software and is designed to enable Cepton's ecosystem partners to integrate and develop solutions tailored for specific markets.

Neil Huntingdon, Cepton's VP of Business Development, says that because the device combines the sensor with a powerful micro-computer in a single package it can process the information directly at the 'edge' and highlight only potential threats, such as an intruder or a suspicious package. This then guarantees the anonymity of those not involved in any suspicious incident.

Said Huntingdon, "Our technology allows for far greater protection of data because it allows operators to zero in on possible issues in a way other technology cannot. Perhaps most importantly it means we can guarantee the anonymity of people or objects not deemed a threat. This is a step-change from existing technology, where everyone's face is captured and held on video storage, regardless of whether they were involved in an incident or not."

Cepton's technology, which can operate over Wi-Fi, mobile networks or Ethernet, can also be used to enable driverless cars and to monitor traffic and infrastructure usage, enabling smarter modelling of transport networks.

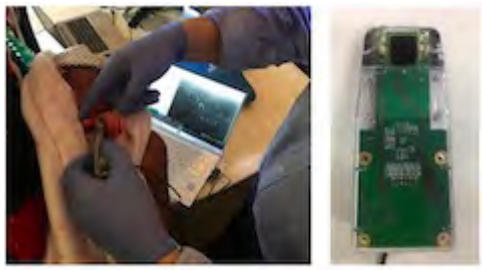
Huntingdon added, "This technology is undoubtedly an exciting prospect for security and transport – and we believe it is the key to the delivery of truly smart cities that can make our communities safer and more connected." SST

Biometric Registration Of Newborn In Kenya

A trial of fingerprinting newborn children from as young as two to 24 hours old in the Republic of Kenya has concluded in June 2019. The trial is expected to help establish a reliable foundation for biometric authentication of newborn children in emerging countries.

The trial deploys NEC's fingerprinting technology, which is designed to cause minimal stress for newborn children after caregivers have provided informed consent to taking their children's biometric data.

Pilot Biometric Registration Of Newborn In Kenya With NEC Fingerprint Technology



Collection of newborn fingerprints ensures proper registration and identification

In order to collect the fingerprints of newborn children within hours of being born, NEC adopted a high-resolution image sensor with a high-resolution imaging element of 10 micrometres, and combined special glass for enhancing patterns. This made it possible to capture high-definition images of 'valley line' patterns of approximately 20 micrometres.

To eliminate blurring due to the movement of newborn children's fingers during the fingerprint capturing process, the frame rate was increased from the previous two frames per second to seven frames per second, and the sensor area was equipped with a blurring prevention function. In addition, NEC adopted specialised equipment that is optimally designed for newborn children, with contours that safeguard children's soft fingers against being pressed strongly against imaging surfaces and guides that ensure the most appropriate direction and position of the finger.

The ability to collect and authenticate biometric information at an early age enables authorities to provide legal identity, including birth registration, for newborn children. This ensures proper identification as they are discharged from the hospital. It also supports the accurate management of vaccination schedules.

The trial is based on field research that began in 2016, which yielded an error rate of just 0.3%.

Today there are approximately one billion people worldwide without legal identity. In addition, an estimated 5.6 million children under the age of five, including 2.6 million newborns, lose their lives each year. Most of these deaths are considered to be from illness that can be avoided through preventative measures and treatments.

To solve this problem, it is necessary to establish methods for registering and identifying newborn children as well as recording their medical history. This is especially important in regions where newborn children are often released from healthcare facilities in as few as six hours after birth. In addition, it is also vitally important to be able to confirm the vaccination schedules of children within 14 weeks of birth.

Moreover, as children grow and mature, this identification system can assist with ensuring that children are placed in schools at appropriate times.

Going forward, NEC aims to provide this technology for practical use within biometric authentication infrastructure and national identity systems in emerging countries throughout the world. SST

Abloy Scoops Coveted US Government Security Award

Abloy USA has been awarded a prestigious Platinum 'Govie' Award for PROTEC² CLIQ Connect. This is the highest-level award available in the 'Access Control Devices/Peripherals – Wireless' category.

Awarded by Security Today, an integrated product and technology magazine for the North American security market, the 'Govies' recognises outstanding government security products.

PROTEC² CLIQ is an access control system based on detainer disc cylinders and electronic identification for double secured access. ABLOY PROTEC², which is based on the patented rotating disc cylinder mechanism, takes care of mechanical security, while the electronic CLIQ technology allows flexible control of keys, access rights and audit trails. PROTEC² CLIQ combines both technologies into one solution.

continue on page 22

In addition PROTEC² CLIQ keys are also available as Connect keys that can be wirelessly programmed using CLIQ Connect smartphone application. This makes it possible to update the user's keys with new access rights anytime, anywhere. The app is ideal for geographically spread out organisations, and the optional personal PIN code authentication added to the mobile key makes it even more secure.

An independent panel of judges from the security industry were responsible for selecting products to receive Platinum and Gold awards.

The PROTEC² CLIQ access control system was conferred the Platinum award because it combines the best of electronic and mechanical locking. The

CLIQ locking system is established globally as an access control and key management solution to protect Critical Infrastructure, with clients including South Staffordshire Water (UK), Helsingin Energia (Finland) and Eskilstuna Energy and Environment (Sweden).

CLIQ has previously been awarded the Merlion Awards 2015 (Golden Winner, Access Control category), Garuda Awards 2012, CTSS Awards 2012, IFSEC Awards 2011 and Merlion Awards 2011.

Aaron Yule, Managing Director of Abloy UK, said: "In the UK, CLIQ is already established as a leading access control solution used in a wide range of sectors to protect critical assets, and this award acknowledges the strengths of CLIQ as a modern, industry-leading access control solution to protect national infrastructure." SST

Victoria Police Supported By Motorola Solutions Managed Service

Motorola Solutions has completed the rollout of a new mobility managed service to Victoria Police, enabling increased situational awareness, safety and productivity on the front line. Officers across the state have received 9,398 mobile devices loaded with smart applications to give them a technological edge while protecting the community.

Motorola Solutions' complete, end-to-end managed service provides the state's police officers with access to real-time information on the beat, allowing them to focus on core policing activities rather than managing the technology. The holistic managed service will run for a minimum of five years with the potential to extend to 11 years and is valued at more than AUD$50 million. The service includes device management, support, repair and replacement services.

The technology delivers immediate operational information to police in the field while helping to preserve mission-critical radio communications for when they are needed most. The solution includes a mobile application developed by Gridstone, the application development firm Motorola Solutions acquired in 2016.

Motorola Solutions Vice President and Managing Director Steve Crutchfield said the rollout allows Victoria Police's frontline officers to have access to data when and where they need it most, so that they can manage essential daily tasks more safely and efficiently.

"For example, the application can provide vital information to officers before they enter a potentially dangerous situation. In the future, the application will also free up officers' time, enabling them to complete crime reporting and administrative tasks in the field instead of back at the station," he said.

Victoria Police are also deploying Motorola Solutions' high-resolution, cloud-based Automatic Number Plate Recognition (ANPR) technology for 220 of its highway patrol vehicles. Motorola Solutions also manages the networks that provide Victoria Police with mission-critical radio communications and narrowband data services. SST

Biometrics Solution PalmID-X Able To Identify Palm From Tens Of Thousands In Under One Second

Palm biometric provider Redrock Biometrics has launched a palm print authentication solution that can identify a palm from a database of tens of thousands in a fraction of a second.

The PalmID-X palm biometric solution expands the capability of biometric identification to large groups of people for seamless services and transactions.

The SaaS matching component is capable of identifying a palm signature from a database of tens of thousands of signatures in a fraction of a second, and biometric data stored in the cloud is encrypted and anonymised without requiring decryption for matching. PalmID-X matching algorithms can also combine facial biometrics, location and text metadata to narrow search results.

"Identification is a much more challenging task than authentication. Most biometric modalities do not have sufficient accuracy for identifying a person in a group larger than a thousand," said Redrock Biometrics Co-founder Lenny Kontsevich. "Palm biometrics is different. It raises the limit more than tenfold from a thousand to tens of thousands."

This expansion in identification capability opens up new applications for identification. For example, frequent shoppers of a supermarket will be able to pay at checkout by merely showing their palm to a payment terminal. There is no more need to carry credit cards or cash.

"Once you register your palm in the system, you hold your identity literally in the palm of your hand," said Redrock Biometrics CEO and co-founder Hua Yang.

Redrock Biometrics' palm print authentication was implemented in Epson's smart glasses platform a year ago, in what was the first biometric authentication solution for a consumer augmented reality headset.

All It Takes Is A Wave Of The Palm To Verify Identification

PalmID-X captures palm prints, subdermal veins, or both, and its proprietary PalmID algorithms match them across a wide range of palm positions, orientations and illumination conditions.

Dirty hands, scars or insufficient light will not prevent palms from being correctly identified, according to Redrock.

The technology utilises the palm of your hand as a secure 'key' to authenticate into a variety of services, online and offline. Just show your palm to the camera from a distance of six inches or more and, in a fraction of a second, you will sign in, authorise a virtual payment, or verify your identity at a bank.

Think of the palm as a very large fingerprint with a rich structure that can be captured by any camera. With PalmID-X, palm images taken with any RGB or infrared camera with a resolution of 0.3 MP or above can authenticate a user in under 100 milliseconds, depending on CPU speed. PalmID uses machine vision techniques to convert the palm image to a unique signature that Redrock says is impossible to fake.

Any device with a camera can use the technology. This includes smartphones, ATMs, desktops and AR/VR devices.

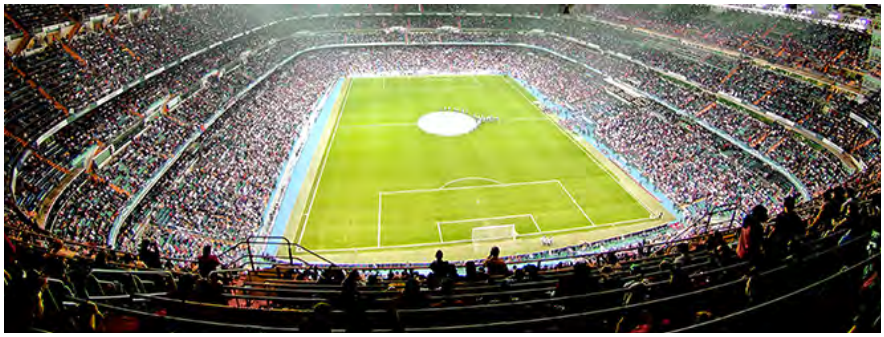
PalmID-X is enrolment portable, enabling fast sign-in for a multitude of platforms like Windows, iOS, Android and Linux. SST

Dallmeier Camera Confirms Identity Of Jeering Juventus Fan

On 3 May 2019, during the derby football match in Turin, a fan of Juventus Turin made offensive reference to the victims of the Superga plane crash.

Soon after the match ended, a video surfaced on social media showing the Juventus fan with outspread arms imitating an aeroplane, mocking the victims of the Superga plane crash. In that tragedy that happened on 4 May 1949, a total of 18 players of rival city football team FC Turin lost their lives. After Juventus Turin was made aware of the existence of the video, security

continue on page 24



officials searched for the man in the video recordings. They were able to identify the man within a day through high-resolution footages supplied by the Panomera multifocal surveillance camera system from German manufacturer Dallmeier.

The culprit has since been banned from the stadium for five years, and the video materials have been released to the police to assist with further prosecution.

Large-scale events are a major challenge. One of the biggest issues is ensuring the safety of visitors at all times. Panomera multifocal sensor systems from Dallmeier have ensured security for Juventus Turin's Allianz Stadium since 2014, as they do in many other football stadiums all over the world.

The main advantage of Panomera systems is that they permanently deliver a complete recording of everything that happens with a defined minimum resolution density, even over very large surveillance areas. At the same time, Panomera cameras are also capable of zooming in on any detail of the entire scene in high resolution – both live and in the recording – and so guarantee identification of individuals for evidence that is admissible in court. This is another significant advantage over conventional solutions that combine megapixel and PTZ cameras. SST

Isorg And Sumitomo Chemical Jointly Developing Organic Photodetectors For Smartphone Fingerprint Sensors

Isorg and Sumitomo Chemical are collaborating to develop new organic photodetectors products for use as smartphone fingerprint sensors and hybrid organic CMOS image sensors.

Isorg, a pioneer in organic photodetectors and large-area image sensors, will license its technology processes to its OEMs, while Sumitomo Chemical, a leader in organic photodetectors materials production, will manufacture the dedicated organic semiconductor material and support Isorg in production technology and marketing.

With this partnership, the two firms hope to provide OEMs with the materials and technology processing solutions that will enable them to bring to market products using high-performance, high-quality fingerprint and CMOS image sensors.

The fingerprint sensors can be incorporated beneath the entirety of a smartphone display, allowing fingerprint recognition from any point or position on that display. The hybrid organic CMOS image sensors are intended for use in cameras, including those designed for near infrared capabilities.

Isorg expects the partnership to yield the leading solution for fingerprint sensors and hybrid organic CMOS image cameras; one that offers significant performance advantages. Both Sumitomo Chemical and Isorg believe the sensors will meet the performance and quality standards necessary for application in the security, automotive, diagnostics and consumer electronics markets.

"Partnering with Isorg will allow us to fill a void in the market for difficult-to-manufacture, but affordable, full-size fingerprint and CMOS image sensors that are suitable for demanding applications in smartphone displays and hybrid visible and near infrared cameras," said Hiroshi Ueda, executive vice president at Sumitomo Chemical.

Sumitomo Chemical and Isorg will work jointly on commercialising the products. SST

Debut Of World's First Blended Hands-On Data Protection Course

Singapore Management University (SMU) Academy and Straits Interactive, a specialist in data privacy, has integrated virtual reality (VR) technology and software tools into their data protection courses, starting with the new Practitioner Certificate in Personal Data Protection (Singapore) Preparatory Course.

Kevin Shepherdson, CEO, Straits Interactive

Developed by the Personal Data Protection Commission of Singapore, this course equips data protection officers with the know-how to establish a robust data protection infrastructure for their respective organisations.

Participants will be using DPOinBox, a customised software designed by Straits Interactive to enhance the effectiveness of their role in implementing the Personal Data Protection Act for their organisations.

DPOinBox delivers data protection as a service (DPaaS) that includes a specialised all-in-one privacy management toolkit and intelligent inbox that allows data protection officers to achieve operational compliance with the Personal Data Protection Act and other data protection laws, including Europe's GDPR. It also enables organisations to implement data protection and data privacy management programmes. In addition to this, the platform makes it easier for businesses to demonstrate accountability to regulators. Any data protection officer can sign up for a Basic DPOinBOX service plan for free.

DPOinBOX comes with online e-Learning modules that allow organisations to create a training campaign and assess staff competency on compliance with various data protection regulations. A tracking report is also available after the campaign is completed so companies can identify staff who need more attention and guidance with training.

"The recent data breaches in Singapore are timely and sobering reminders of the vulnerabilities that organisations face. As such, we have been working with Straits Interactive to explore new ways of encouraging data protection officers to get themselves trained adequately, and to comply with the Personal Data Protection Act, not just for legal reasons but to enhance and strengthen their operations," said Dr Lim Lai Cheng, Executive Director, SMU Academy.

"From the start, our DPO courses were designed to impart to participants practical and relevant knowledge; the newly incorporated VR technology will further engage participants and make their learning experience richer and more impactful," she added.

Said Kevin Shepherdson, CEO, Straits Interactive, "Complying with the Personal Data Protection Act operationally means taking an inventory of personal data that an organisation collects and holds, charting its flow from collection to disposal, and carrying out a data protection impact assessment to determine risks. For a newly appointed data protection officer, this process is likely to be overwhelming if done manually or with spreadsheets. Hence our decision to introduce the blended learning approach to this course."

Participants will be provided with VR headsets to fully immerse themselves in a 360 degree environment while they identify potential data breaches in real time. The high-level technology enhances staff awareness on how data protection breaches can occur, so they can take measures to remedy their workplace. In the courses, participants are asked to identify data breaches and input them into the software's risk register so that follow-up action may be taken.

Said Shepherdson, "It's one thing to read about data breaches from notes and slides or through video clips. We have found it's a completely different lesson when participants can experience a data breach in an immersive 3D environment."

Over 500 organisations from all industry sectors have attended the blended learning courses since they first began. The majority of the participants are data protection officers, legal counsel and compliance managers.

SMU and Straits Interactive plan to roll out the blended learning approach to all 14 data protection related courses being offered at the SMU Academy. SST

New RDC Singapore Office To Fight Financial Crimes

RDC, the global leader in compliance screening, announced that it is opening an office in Singapore to serve and build the company's presence in the Asia Pacific region.

RDC's Singapore office will serve as the centre of the company's activities in the Singapore market and the broader Asia Pacific region, supporting RDC's continued growth while also helping maximise the company's ability to serve both new and existing clients in Singapore, Hong Kong, and other Asia Pacific countries.

Founded by 20 of the world's leading financial institutions, RDC prevents criminal infiltration of the world's financial systems by delivering automated, intelligent customer screening and decision-ready intelligence. RDC supports more than 1,000 organisations and 35,000 compliance professionals across more than 100 countries in strengthening their Know Your Customer and Anti-Money Laundering Checks, fraud and Politically Exposed Persons protection, ensuring sanctions and watchlist compliance, protecting their brand and reputation and managing supply chain and vendor risks.

The office opening coincides with the launch of the FinTech FinCrime Exchange Asia, in which RDC serves as a corporate partner. FFE brings together a global network of FinTechs to collaborate on best practices in financial crime risk management.

Both launches are a result of Singapore's significant and growing FinTech market, as well as the region's large pool of major banking and financial service providers. Singapore's status as a centre for both emerging and established financial institutions makes it an ideal setting for RDC expansion. SST

MIT Technology Review Lists Huawei Among 50 Smartest Companies

Huawei was named one of the 50 Smartest Companies by MIT Technology Review in June. Huawei was included in the list this year for its outstanding capabilities in innovation.

The MIT Technology Review is a globally influential technology media outlet that annually publishes a list of the 50 companies that best combine innovative technology with an effective business model around the world.

Each year MIT Technology Review picks the 50 smartest companies based on what the companies did over the last year, what methods they used and what achievements they made. The magazine evaluates the companies' core competence with emerging technologies and any breakthroughs

William Xu, Huawei's Director of the Board and President of the Institute of Strategic Research, speaking at the 50 Smartest Companies 2019 China Summit

continue on page 27

Awarding Ceremony at the 50 Smartest Companies 2019 China Summit

and innovation the companies have achieved for themselves, their industries or even the world.

Said William Xu, Huawei's Director of the Board and President of the Institute of Strategic Research, "Over the past 30 years, Huawei mainly made technical and engineering innovations as well as innovations in solutions based on customer needs. We call that Innovation 1.0. In the future, Huawei will pursue Innovation 2.0, which refers to theoretical breakthroughs and inventions driven by vision. Huawei sticks to open innovation and inclusive development. Open innovation means innovating together with global experts. In this process, resources and capabilities are shared. Inclusive development means the fruits of any innovation should be shared and used by all humanity and industries. This can lighten the future of the world and industries."

William Xu added that Huawei will continue to support the research of universities and institutions, and is committed to exploring and identifying future-proof technologies along the whole information process, from information generation, storage, computing, transmission, and presentation to information consumption.SST

Do you have news for us?
Good! Email us at sst@tradelinkmedia.com.sg

Keeping An Eye On Caravaggio

Photos courtesy of Bosch Security and Safety Systems Global

From renaissance to pop art, from Caravaggio to Rauschenberg, El Museo Thyssen-Bornemisza in Madrid features some of the world's finest pieces of art.

Bosch is contributing to making sure these artworks stay where they belong by helping the museum switch from analogue video surveillance to an IP-based system.

With this switch, Bosch is creating a single integrated security system, allowing the museum to receive and monitor all alarms centrally. The new system replaces the existing equipment with new IP cameras for the museum's different exhibition rooms and provides recording and storage of images and video analytics. The complete security installation is managed by a Bosch Video Management System.

"Since the video system is equipped with an iSCSI redundant recording solution, the system stays operational even if any of the recorders are temporarily lost. With this new setup, the main benefit is that we have a backup system for our recordings that provides a reliable, efficient security system."

- Miguel Ángel Molina, Security Manager

Eliminating Blind Spots Using Fisheye Lenses

Bosch IP panoramic cameras were chosen by the museum for its Temporary Exhibitions Room to maintain a watchful eye on each art installation and to eliminate blind spots. These cameras featuring a 'fisheye' lens provide a full 180- or 360-degree overview of an area. The camera's built-in dewarping functionality transforms the circular image into distortion-free rectangular images that can be easily viewed in high resolution thanks to its 12-megapixel sensor.

The chosen Bosch IP panoramic cameras have built-in Intelligent Video Analytics, which continuously analyses all video images. If a pre-defined scenario is detected, an alarm is triggered. Intelligent Video Analytics continues to monitor the full image circle so that the user continues to receive alarms even if the security personnel decides to zoom in on a particular region.

Full Situational Awareness With Special 'Museum Mode'

As an optional feature, a special 'museum mode' enables the museum's security to predefine a perimeter around an artwork and to create a virtual, invisible protective barrier. If an individual breaches this perimeter in an attempt to touch or steal the artwork, an alarm is triggered and immediately received both in the control centre as well as by the security personnel on their mobile devices, allowing them to react and take action quickly. This virtual barrier is a convenient alternative to conventional infrared barriers.

Additionally, for exhibits displayed in low light conditions such as the recently exhibited Bulgari and Rome in the museum's Moneo Room, the Thyssen-Bornemisza Museum selected Bosch IP 6000 series cameras featuring the latest starlight technology. Bosch starlight IP cameras are made for low light conditions, providing high quality colour images in almost complete darkness.

Reliable And Efficient Setup

The museum's Security Manager Miguel Ángel Molina expects to incorporate more technologies and innovations for security and protection in the following months. "Since the video system is equipped with an iSCSI redundant recording solution, the system stays operational even if any of the recorders are temporarily lost. With this new setup, the main benefit is that we have a backup system for our recordings that provides a reliable, efficient security system." SST

Record Vulnerabilities Spark Cybersecurity Innovation Among Global Enterprises

New data ranking the 'cybermaturity' of organisations reveals the most commonly targeted sectors are also the most prepared to deal with the ever-evolving threat landscape

According to NTT Security's 2019 Global Threat Intelligence Report, globally the average cybersecurity maturity rating stands at a worrying 1.45 out of 5 – a score determined by an organisation's holistic approach to cybersecurity from a process, metrics and strategic perspective. This comes during a time when security vulnerabilities have also surged to a record high (up 12.5% from 2017).

The finance (1.71) and technology (1.66) sectors boast the highest maturity ratings and are continuing to ramp up their security posture, most likely prompted by their unenviable positions as the most commonly targeted industries, each accounting for 17% of all attacks recorded in 2018.

Scouring trillions of logs and billions of attacks, the research also revealed the most common attack types, with web attacks the most prevalent threat, doubling in frequency since 2017 and accounting for 32% of all attacks detected last year. Reconnaissance (16%) was the next most common hostile activity, closely followed by service-specific attacks (13%) and brute-force attacks (12%).

Neville Burdan, Solutions Director-Cybersecurity at Dimension Data Asia Pacific, said, "There's clearly work to be done across all sectors in order to establish more robust security postures. However, it's reassuring to see many C-suite leaders recognising the importance of making more strategic investments to improve their cybersecurity defences."

He continued, "There have been some exciting developments in the predictive threat intelligence space, with new levels of collaboration and buy-in across the cybersecurity value chain. What's more, the most-targeted industries are also the most likely to seek assistance to evolve their strategies and build their security programmes. This bodes well for companies looking to reach their desired cybermaturity state."

Other highlights from the research include:

- Globally, 35% of attacks originate from IP addresses within the US and China, followed by EMEA and APAC.
- Cryptojacking represents a significant amount of hostile activity, at times accounting for more detections than all other malware combined, hitting the technology and education sectors hardest.
- Credential theft is up as attackers target cloud credentials, with tech companies (36%), telcos (18%), and business and professional services (14%) significantly impacted by this. SST

CCTV Cameras In London Projected To Hit One Million By 2025

Exactly how many security cameras are there in London right now? According to an estimate by CCTV.co.uk, the answer is 627,000.

CCTV.co.uk is an installer and service agent of close-circuit television systems for businesses and homes in the United Kingdom.

This all-time high figure translates to one camera for every 14 people in London, and takes into account CCTV fitted to both commercial properties and private households. Such a huge increase in the number of CCTV cameras in recent years means that anyone going about their business in the capital will be caught on camera around 300 times per day.

London is one of the most heavily surveilled cities on earth with some of the most surveillance cameras per head of population in the developed world. London is often referred to as the CCTV capital of the world.

The vast majority of CCTV cameras are operated by private individuals and businesses rather than government bodies and such privately operated closed-circuit TV cameras must only be logged with the Information Commissioner's Office if they're not used for domestic purposes such as monitoring the security of property.

But what's driving this rapid growth in surveillance?

Jonathan Ratcliffe, spokesman of CCTV.co.uk, attributes this to a combination of increased fear among householders, the standardisation of commercial security in new buildings and the smaller affordable security cameras such as home CCTV Systems and Doorstep Cameras.

Ratcliffe said: "The number of cameras being installed in the capital is growing at a much faster rate than ever before due to private households installing smaller cheaper systems."

In its 2015 report **The Picture Is Not Clear: How Many CCTV Surveillance Cameras Are There in the UK?** the British Security Industry Association suggested that camera numbers in the private sector could outnumber those used by public bodies by as much as 70 to one.

Explained Ratcliffe, "People are genuinely scared and sharing CCTV footage on social media when the police don't act fast enough is standard practice these days. Doorbell cameras and cheap DIY systems have seen the number of cameras increase, and new commercial buildings have CCTV installed as standard."

And this growth isn't set to stop anytime soon. CCTV.co.uk anticipates that by 2025 there will be one million cameras in London alone, reflecting a growing trend that's also mirrored around the country.

Said Ratcliffe, "We estimate one camera for every 14 Londoners, but this could rise to one in 11 as technology improves and population increases, meaning a staggering one million cameras by 2025." SST

A Look Back At The First Year Of GDPR

It has been almost a year since the implementation of The EU General Data Protection Regulation (GDPR) for businesses in Europe. However research shows 62% of organisations were still not compliant as of March 2019. We capture the first year of GDPR in infographic and get some answers on GDPR from security experts from Synopsys.

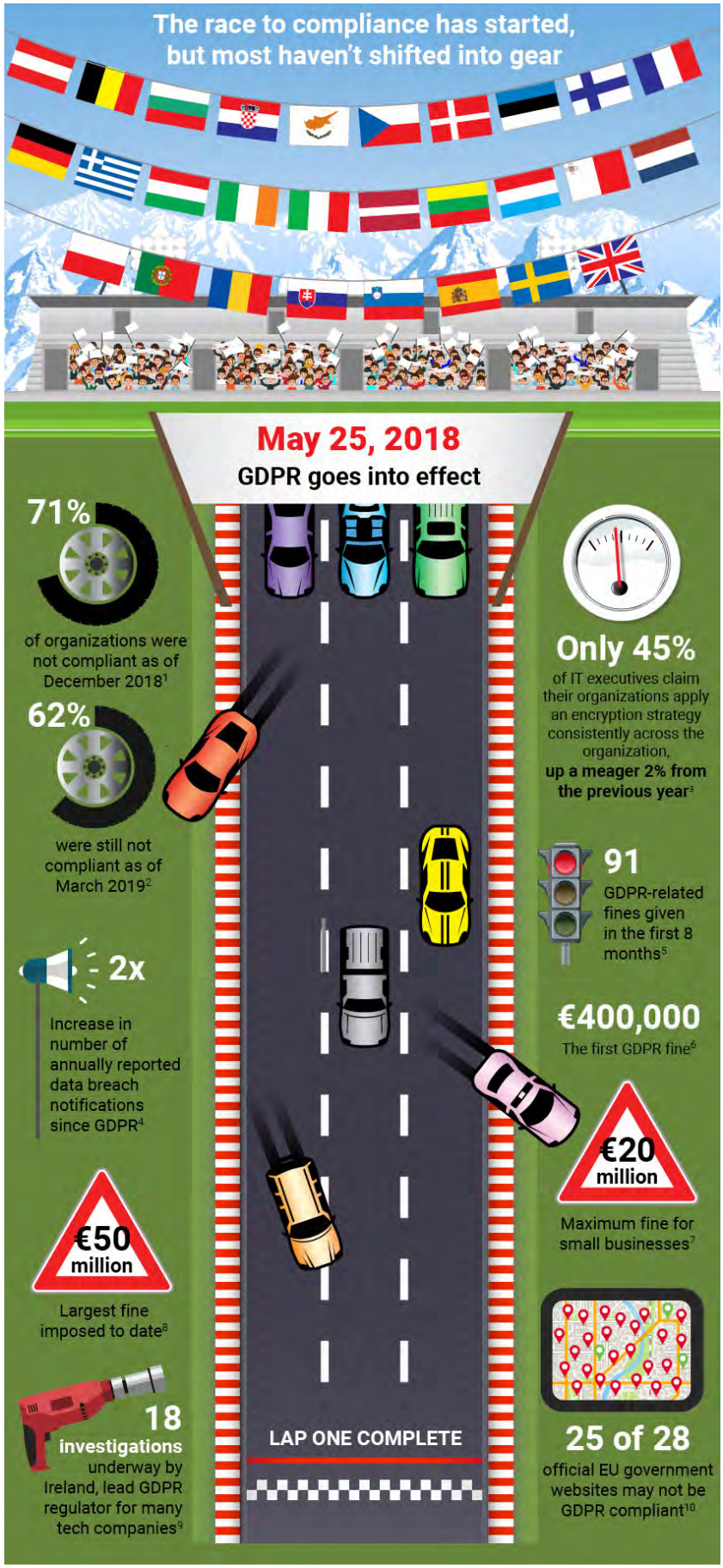
Q: What are businesses' obligations under GDPR?
Synopsys: The single most important obligation under GDPR is for an organisation to recognise data privacy is now mandatory and proper management of data collection and processing can only occur under dedicated guidance. That means the appointment of a data protection officer familiar with the nuances of GDPR. Critically, organisations headquartered outside of the EU should recognise GDPR enforcement isn't based on where an organisation primarily operates but on how it handles data of EU residents.

Q: Does GDPR apply to international businesses?
Synopsys: Absolutely. Regardless of your organisation's location, whether it operates primarily inside or outside of the EU, if your organisation uses data relating to EU residents, then GDPR applies to you. Transactions include operations carried out by employees, other organisations' data and customers — even those receiving a free service. While it might be tempting to assume that if your organisation operates only in a specific region outside of the EU that no GDPR obligations exist, the reality is that if your organisation interacts with an

EU resident and collects data during that interaction, then GDPR is something you need to be aware of.

Q: Who does this policy affect? Only EU citizens?
Synopsys: GDPR directly impacts how businesses process the private data of EU residents. Private data is defined within the directive, and importantly businesses must have a legitimate reason to collect or process that data. This concept is referred to as 'lawful basis' and doesn't include an option of "because we wanted to do something cool with that data". For most organisations the four valid options for lawful basis include: consent, contract, legal obligation and legitimate interests. In the case of consent, consent must be granted prior to data collection and, importantly, can be revoked at any time. The legitimate interests option might on the surface appear the most flexible of choices, but it is also open to concepts such as reasonable expectations. For example, when using the legitimate interests option, the proposed collection and processing options must be within the realm of what a normal user might expect and be necessary to the delivery of a service.

Q: Can I turn GDPR risk into a competitive advantage?
Synopsys: The primary business advantage of comprehensive GDPR implementation is customer goodwill. Reputational and brand damage occurs when data breaches are disclosed. Following a data breach, business operations will be impaired for months (if not longer) while security and regulatory oversight weaknesses are addressed. This is before any fines or sanctions are imposed. As we've seen with the Commission nationale de l'informatique et des libertés' (CNIL) €50 million judgement against Google earlier this year, fines can be substantial but GDPR applies to how products are designed and businesses operate, not just how organisations respond to a data breach. SST



How To Avoid Getting Hooked By Mobile Phishing

►► **By Brian Gleeson,**
Head Of Mobile Security Product Marketing, Check Point Software

The first recorded use of the term 'phishing' was in 1996, in the earliest days of the Web. So why is this over 20-year-old method of online fraud still with us? For one very simple reason: it works very effectively. It's one of the most reliable methods a hacker can use to steal access to personal or business digital accounts. The FBI estimated that the total losses from business email compromise alone – a highly targeted variant of phishing – have exceeded US$12 billion globally. Phishing has become an industrialised process. It's estimated that around one in every 2,000 emails is a phishing email, and over a million fake websites are created every month to try and trick users into giving away personal information. A recent study showed that 25% of phishing emails bypass Microsoft Office 365 security.

For criminals, it's a numbers game: they just need to distribute enough emails and links to fake sites and wait for people to fall into their traps. And as more and more transactions are conducted via mobile devices, mobile users are being increasingly targeted – with increasing success.

There are several reasons for the rise in mobile phishing attacks. First, the ergonomics and smaller screen size of mobiles makes it harder for users to inspect an emailed URL that they are asked to click on – and easier for scammers to attract unwitting visitors to their fake sites. Second, mobile devices are typically used to connect to multiple email accounts, enabling hackers to target both business and personal accounts. And finally, smartphones can also be targeted by phishing texts and malicious apps, giving the attacker a range of methods to try and get victims hooked. Let's take a closer look at each of these three main phishing vectors.

Spear Phishing By Email

Email phishing attempts can target both consumers and enterprise mobile users. Spear phishing attacks on consumers usually involve stolen databases of consumers' names, phone numbers and accounts to create very targeted and convincing messages. For example, hackers will use a stolen database of credentials from a major breach – such as the recent breaches at Equifax or Yahoo! — to send mobile users targeted messages using that brand's name or personal information about the recipient.

Attacks against enterprise users involve building a profile of individuals from corporate websites and LinkedIn, Facebook and Twitter profiles, and then creating targeted emails that purport to be from a senior executive, requesting an urgent payment or service and directing the target to make a legitimate-looking but fraudulent transaction. Alternatively, these attacks can appear to originate from the enterprise IT team, directing users to URLs to collect passwords and VPN credentials.

SMS Phishing

So-called 'smishing', SMS, text and iMessage phishing is an increasingly common vector for delivering malicious URLs to mobile device users. Again, there are several varieties, from large-scale attacks resembling spam email attacks that incorporate ruses such as password resets or account security updates, to far more targeted and personalised attacks.

App Phishing

Mobile apps have become a hugely fruitful channel for the distribution of phishing links. After all, most mobile devices have a huge number of apps installed, and with over 3.8 million apps available to Android users on Google Play, over two million apps on the Apple App Store, and over 1.5 million apps on other third-party stores, there are plenty of opportunities for hackers to introduce malicious content.

Yet again, there are multiple varieties to be aware of. Encrypted communication phishing takes advantage of the encrypted nature of WhatsApp, Telegram and Signal to send convincing messages claiming to be from customer support or a known online service, which cannot be flagged by the enterprise because they are encrypted.

Fake social media phishing uses apps like Twitter, with attackers setting up fake accounts purporting to be genuine customer support services. And of course, there are entirely fake apps, and even fake third-party app stores. The latter often use the technique of distributing a configuration profile that is installed on a device by visiting a web page. Once such a profile is installed on the mobile device, the user can then access the third-party app stores and download apps to the device. These apps are not subjected to any verification or security review, and can be used to deliver phishing URLs, malicious content and even to install malicious apps on the user's device.

Next-Generation Protection Against Being Phished

To protect individuals and organisations against phishing attacks, a four-stage approach is needed.

1) The first line of defense is robust, server-based anti-phishing protection. This must incorporate anti-spam filtering, phishing detection, BEC phishing detection and spear phishing detection.

2) Second, device-based URL protection is a must, given that the vast majority of phishing attacks direct a victim to a URL that provides convincing content to trick the user into disclosing credentials or installing malicious apps. URL protection that spans not just an enterprise email account but also personal email accounts, SMS/text/iMessage and the content that apps download is crucial.

3) The third stage is device-based security profiling, in order to detect whether devices have been purposely or inadvertently made vulnerable to targeted attacks or traffic interception. This requires examining operating system versions and patch levels, installed configuration profiles and certificates, and scanning for malicious apps.

4) Finally – and this element is often neglected – user education is essential. The nature of phishing attacks requires unwitting or uneducated users at the device side and even the most sophisticated technical education can be undone in a second by a careless user. And as mobile phishing attacks get more sophisticated, with sophisticated social engineering techniques mobilised to trick even savvy individuals, user education has become even more important.

Workforces need to be educated to be suspicious of any email that is unknown, to avoid opening any attachment that is not known or requested, to not provide any personal information over email or text, and to exercise extreme caution when they receive unexpected payment notifications via email or requests from social media contacts they don't recognise.

They also need to be able to identify potentially fake websites, and know to immediately close their browser if a URL directs them to a completely different website.

With this combination of best-practice security technologies and user education, organisations will be in a good position to ensure that their employees do not easily fall for the bait offered by mobile phishers. SST

Password Strategy: What Makes Your Users' Passwords Exploitable

►► **By Nabil Hannan,** Managing Principal at Synopsys

Passwords are the gatekeepers to our most sensitive information. They serve as the first line of defence against a potential intruder, but they are not bulletproof.

As users, we're tempted to create passwords that are easy to remember - by using birth dates or anniversaries, for example - and even writing them down. As developers, we're tempted to put as little time into our password strategy as we can.

Unfortunately, these passwords are very weak and guessable and leave us wide open for an attack. Worst of all, the systems that we trust to store this critical information face plenty of security challenges too. Hackers have identified password databases as ripe and easy targets for theft, and concerted attackers can almost always defeat the schemes by which those database are protected.

Let's look at some common errors that companies make with their password strategy.

1. Your password strategy hasn't changed in 10 years

Attack: Once an attacker steals a cache of stored passwords, they begin reverse-engineering its protection scheme. Password storage mechanisms are simply a barrier to attackers — one that slows them down, but does not stop them.

Defense: When you store passwords, you can and should implement further protections to serve as barriers. Think of them as speed bumps, but set the speed bump too high, and you run the risk of annoying your users — and overtaxing your server.

Remember: No matter how high you build your barrier, attackers will ultimately be able to overcome it. The ongoing challenge here is to design your password storage to slow down attackers while also balancing the needs and satisfaction of your users.

2. You've limited the number or variety of characters users can use

Attack: Brute force attacks occur when an attacker attempts to discover a password by systematically trying every possible combination of letters, numbers and symbols until they uncover the correct combination that works. When users choose guessable passwords ('password1' anyone?), it makes a hacker's job easy.

To further simplify the process, hackers use tools that utilise wordlists and smart rulesets to intelligently and automatically guess user passwords. Some organisations restrict the type of special characters and the

When you store passwords, you can and should implement further protections to serve as barriers. Think of them as speed bumps, but set the speed bump too high, and you run the risk of annoying your users — and overtaxing your server.

length of credentials accepted by systems because of their inability to prevent SQL Injection, cross-site scripting, command-injection and other forms of injection attacks. These restrictions, while well-intentioned, facilitate brute force attacks.

Defence: Do not allow short or no-length passwords and do not apply character set or encoding restrictions on the entry or storage of credentials.

3. You're storing passwords in cleartext

Attack: Storing passwords in a database in cleartext opens up a variety of risk factors that can compromise an application. In telecommunications, cleartext is a message or data presented in a form that is immediately understandable to a human being without additional processing. In other words, this message is sent or stored without cryptographic protection. There are several ways an attacker might be able to gain access to the database through SQL injection or exploits, or by stealing the backup disk. If the attacker succeeds, he or she can access all user accounts and read all user passwords that are in cleartext.

Defence: Cryptographic hashes like those in the SHA family slow down those attacks. But they are not invulnerable. Attackers equipped with fast hardware can still easily crack these passwords.

A rainbow table is basically a pre-computed set of plaintext strings and their corresponding hashes. They are 'optimised lookup tables' that are publicly available that can be used to reverse engineer one-way hash functions. Attackers can use one of these tables to retrieve cleartext data that has been hashed.

4. You're using hashes that produce collisions

Attack: Hashes enhance the security of password storage, but they are not fail-safe. Hash algorithms can suffer from several different kinds of cryptographic attacks, such as collisions. A collision is when two distinct inputs result in the same hash digest. Good hash algorithms are designed to be collision-resistant, but they are impossible to eliminate completely.

Defence: Use SHA-256 to produce longer hashes that avoid known collisions.

5. You're not salting your passwords

Attack: In any password system, it is possible that two users may use the same password. An attacker who identifies the duplicate passwords can use the known password to authenticate as any user whose hash matches, or can use that information to crack the system using dictionary chosen plaintext attacks.

Defence: Salts prevent collisions by adding random data to each plaintext password. Use salting to make two previously identical plaintext passwords differentiated in their enciphered text form, so that duplicates cannot be detected. Random salts also add entropy to input space and make lookup tables larger.

Conclusion: Design For Failure

While there is no fail-safe way to store passwords, it is important to design your password storage with the thought that it will eventually be compromised. Add these alternative credential validation workflows to your password strategy for an added layer of security:

Protect the user's account:

- Invalidate authentication 'shortcuts' by disallowing login without second factors, secret questions or some other form of strong authentication.
- Disallow changes to user accounts such as editing secret questions and changing account multi-factor configuration settings.
- Support dual authentication with apps such as Duo.
- Load and use new protection scheme.
- Load a new, stronger credential protection scheme.
- Include version information stored with form.
- Set 'tainted'/'compromised' bit until user resets credentials.
- Rotate any keys and/or adjust protection function parameters such as work factor or salt.
- Increment scheme version number.

When user logs in:

- Validate credentials based on stored version (old or new); if older compromised version is still active for user, demand second factor or secret answers until the new method is implemented or activated for that user.
- Prompt user for credential change, apologise and conduct out-of-band confirmation.
- Convert stored credentials to new scheme as user successfully logs in. SST

Artificial Intelligence And Video Technology: Four Things To Keep In Mind

Hardly any topic is creating as much excitement as artificial intelligence (AI) at the moment. High expectations and extravagant promises abound, particularly in the field of video security technology. Ideas about what it can do range from detecting attacks on individuals and recognising individual faces in large crowds of people to automatic detection of the bomb in a suitcase.

Dallmeier, a provider of network-based video security solutions, has been working on and with AI technologies for years. And it has four pieces of advice to offer on the subject of AI and video technologies solutions.

#1 Much more than just technology needs to be considered. When innovations are being introduced, people often ignore the fact that new technologies always require public debate and changes to very real framework conditions before they can be implemented wholesale.

Today unresolved issues remain on how AI is to be used in video security technology,

The questions include: How much freedom should a system be given? What quality criteria will be established for detecting objects? Who is to be held accountable when an attack is not detected, for example, even though the expectation may possibly exist already among the people? What reaction times will be defined? By when must response teams reach the site in the event of an 'AI alarm'? Are there even

Dallmeier, a provider of network-based video security solutions, has been working on and with AI technologies for years. And it has four pieces of advice to offer on the subject of AI and video technologies solutions.

enough personnel available for the potential new intervention and search options? How are the many ′false positives′ to be handled when facial recognition is used to find a suspect?

#2 AI and video technology only function in a ′technologically holistic approach′.

Technical systems are becoming more and more complex. This is why it is essential to evaluate all of the parameters that affect the performance of a whole solution. The IT axiom ′garbage in, garbage out′ is most apposite in this context.

Neural networks for classifying objects and processes and good facial recognition software will deliver results that accord with the quality of the video image they receive. AI-based video analysis systems can only be as good as the camera systems that capture the images for them.

It is important to define and plan minimum picture qualities properly in all parts of the video image, plan camera angles correctly and consider many other details. And the person behind the system must also be included in the overall consideration with regard to qualification and organisational questions.

In short: unless all factors are tuned to work together, it will not be possible to ensure compliance with standards – which by the way have not even been defined yet!

#3 AI in video technology currently takes on the function of a useful assistance system. It goes without saying that AI will play a decisive role in video technology. It may even become a core component of the discipline.

Functioning solutions already exist, whether it be in the optimisation and analysis of analogue processes (such as at a casino gaming table), in the improved classification of objects for perimeter protection, or in the assisted tracking of individuals in the context of urban surveillance. The key point in all of these systems: a human is still at the centre, whether he is the operator, the policeman or the forensic specialist. Today and probably for a long time to come, AI in video technology will serve the function of enabling useful assistance systems.

#4 Learn to distinguish between functioning solutions and research projects. It is important to examine and question closely which functions are market ready and implementable and what is still purely in the realm of research. Prospective users should always begin by asking themselves whether a given result can be expected in 12 months, five years, or ever. Otherwise, they risk losing sight of obvious solutions to pressing problems. SST

Risk Management: Managers Are Setting The Wrong Priorities

To what extent are risks taken into account in a business strategy?

Operational risks cover all threats that often result in unexpectedly high financial losses. These include supply chain disruptions, fluctuations in production, legal risks and human error. What is important is that managers can effectively prevent these risks. The causes of these risks are normally flawed internal processes and a lack of control mechanisms.

In 2018, consulting firm DuPont Sustainable Solutions interviewed senior managers from various high-risk industries such as oil and gas. The results of the study suggest that many managers set the wrong priorities.

It Just Takes One Single Serious Incident

According to the survey, managers don't allocate enough resources and have insufficient skills to effectively manage risks at their organisations. A key problem is that executives and their managers often just look at the number of incidents at their company to date. This is usually low and creates a false sense of security. In fact it only takes a single serious incident to cause devastating damage.

"In today's global business environment, old methods for assessing operational risks are inadequate for executives in ensuring the sustainability and success of their businesses," explains Davide Vassallo, Global Managing Director of DuPont Sustainable Solutions.

Operational risks are difficult to quantify. In most companies, they can only be recognised through risk assessments by management and internal auditing. The study shows that managers generally consider risk management to be important. However, only 38% of them actually consider it to be part of their corporate strategy.

According to the study, decision makers and management teams urgently need to set new priorities and integrate more suitable risk mitigation measures into their daily processes. Leadership cannot be content with business success alone.

Different Risk Perceptions The Biggest Hurdle

Another critical finding of the survey is that different managers assess company risks differently. Around 55% of those surveyed agree with this statement. The authors of the study believe this makes it difficult to effectively identify and minimise risks.

DuPont also examined what operational risks executive boards discussed most in meetings. This serves as an important indication of risk perception and what companies see as priorities. The result was that topics relating to finance, health, the environment and compliance are frequently on the agenda. Plant reliability, process safety and the supply chain receive less attention. This is despite the fact that interruptions in production or the supply chain due to a fire, for example, are a common cause of damage with wide-reaching consequences.

> ***In today's global business environment, old methods for assessing operational risks are inadequate for executives in ensuring the sustainability and success of their businesses.***
>
> *– Davide Vassallo, Global Managing Director of DuPont Sustainable Solutions*

A New Approach: Proactively Tackling Operational Risks

The authors of the survey advise that management should identify performance trends in advance rather than respond to events and incidents when they happen. A forward-thinking approach to risk is the key to successful business development. In this way, decision makers can involve their employees in their risk prevention strategy, boost productivity and increase their company's competitive edge. If managers don't do this, operational risks could continue to negatively impact business performance, according to the study.

HIMA, provider of safety-related automation solutions, also advise that business leaders should view lifecycle management as a continuous process to ensure plant availability across every phase. HIMA's safety experts recommend regular security checks to strengthen a company's cybersecurity. Plants are becoming more complex and automated controls are prominent in all industries. For this reason, employees require comprehensive expertise. Managers must therefore be aware of what business risks affect the enterprise and not rely on old strategies and data.

Tips On Conducting Security Checks

Kenneth Kng, Regional Marketing Manager at HIMA Group, suggests that organisations conduct four classes of security checks. They are:

- Basic checks that cover documentation and organisational procedures
- Safety instrumented system (SIS) checks covering configuration and application
- PC checks covering SIS engineering and OPC server
- Network checks covering network infrastructure and components

All checks must adhere to IEC 62443/ IEC 61511 Ed 2, IEC27000 and NA 163 standards. SST

Undetected Unauthorised Activity In Critical Systems Is #1 Cybersecurity Risk For Utilities Sector

The utilities industry is rapidly modernising its infrastructure, adding more digitised equipment and connectivity across devices, plants and systems. Unfortunately, the security policies of many utilities have not evolved along with it, leaving them incredibly vulnerable, according to market-foresight advisory firm ABI Research.

ABI Research projects that the industry will spend US$14 billion a year between 2018 and 2023 — a total of US$84 billion over that time period. While investments in digital infrastructure will remain very high over the next several years, investments in securing that infrastructure will lag behind.

This means a growing gap between threats and spending — only 55% of the total security spend in the next five years will be spent on securing smart infrastructure. By 2023, connected utility infrastructure will have essentially doubled in size, exposing utility companies to a myriad of cybersecurity risks.

In its new whitepaper, **The 6 Biggest Cybersecurity Risks Facing the Utilities Industry,** ABI Research identifies the six most prevalent security weaknesses in the Utilities Industry for CIOs and CTOs and offers best practices to utility companies looking to steer clear of cybercriminals and threats.

The most pressing risks are:

1. Boundary Protection (undetected unauthorised activity in critical systems)
2. Physical Access Control (unauthorised physical access)
3. Allocation of Resources
4. Least Functionality (increased vectors for malicious party access)
5. Identification and Authentication (lack of accountability and traceability)
6. Account Management (compromised unsecured password communications)

As these threats continue to mount, it's imperative for companies within the utility space to deploy secure IT/OT solutions. SST

The DNA Of A Systematic Automotive Failure

►► **Matan Scharf,** Senior Security Solutions Manager at Synopsys Software Integrity Group

With so many exaggerated Hollywood depictions of car hacking scenarios, it's easy to imagine a future in which cars are hacked by criminals or terrorists and used as weapons. While there are reasons why such scenarios haven't yet taken place, could they? And if so, how can we prevent them?

While some may argue that the likelihood of cars being used as weapons is quite low, from a technical standpoint there isn't really anything stopping attackers who invest the time and effort from succeeding.

Modern cars are controlled by computer systems, and the most fundamental property of a computer system is the software that governs the operation of the device. Software is inherently susceptible to a wide variety of threats and vulnerabilities. Under the right conditions, any system may be compromised, and its behaviour altered.

Traditionally vehicles are understood to be isolated mechanical machines powered by fossil fuel and controlled by a human. However this definition is evolving as the technology powering vehicles evolves. Advancements in technology over the past 20 years have led to a substantial change in the definition of what a vehicle actually is.

Modern vehicles can be described as electric, connected, software embedded, driverless and even artificially intelligent in some cases. If they're left unmanaged and without security mechanisms in place, such properties render risks that manifest as software bugs and design flaws that could allow unauthorised remote access. As vehicles become more connected and as software continues to spread to more safety-critical systems, these bugs and flaws present an opportunity for catastrophic failure with devastating effect on humans.

If we examine this threat at scale, smart, connected autonomous cars could be a widespread weapon of mass destruction. Thankfully, the automotive industry isn't oblivious to these risks. Far from it. Regulatory bodies have drafted legislation, standards and compliance requirements designed to prevent such failures. And yet compulsory compliance requirements haven't been enough to prevent some of the most notorious breaches and data leaks we've seen in recent years.

The Ponemon Institute recently released a report commissioned by Synopsys and SAE International offering a comprehensive look into the core reasons for these issues and factors contributing to them. It highlights a lack of skills and resources, an inability to communicate risks effectively to management, time-to-market constraints that take priority over software quality, and more.

Let's now take this examination one step further and look into the DNA of automotive companies to articulate the challenge at its core: the reality of vehicle production.

Historically, automakers have been experts in designing and managing the production of vehicles in high volumes under strict quality and safety requirements. In this case, 'quality' was mostly a question of luxury, performance and comfort. 'Safety', on the other hand, was defined and measured as a derivative of collision tests, fault tolerance, and other attributes reflecting the vehicle's ability to protect the driver, passengers and surrounding pedestrians from injury in an accident. This paradigm was deeply embedded into the design, production and manufacturing processes of vehicles.

Everything changed with the emergence of cyber considerations. While this change didn't happen overnight, it wasn't announced ahead of time so that the industry could plan accordingly. Rather, over the past 20 years, vehicles have gradually become attack targets. The definition of safety has become a derivative of secure software development practices, while quality has become the ability to enforce quality downstream in the software supply chain.

In order for car manufacturers to produce safe and secure vehicles, the software code governing the systems operating the vehicle and its various elements must be written with security considerations. For instance:

- The networks connecting components to one another and to the outside world must be separated, segregated, demilitarised, encrypted and fire-walled.
- Systems must be continuously monitored for anomalies.
- Applications and communication must be whitelisted.
- External entities must be authenticated and verified.

The list goes on.

Modern cars are controlled by computer systems, and the most fundamental property of a computer system is the software that governs the operation of the device. Software is inherently susceptible to a wide variety of threats and vulnerabilities. Under the right conditions, any system may be compromised, and its behaviour altered.

From Bad To Worse To Catastrophic

Many automotive companies view these notions as somewhat foreign. As the Ponemon research indicates, most organisations do not have the right talent pool, experience and infrastructure to address these challenges. The gap isn't limited to technical knowledge in the workforce and budget allocation. It also exists in the organisation's ability to adopt the mindset needed to function in a hostile environment where malicious actors operate and software bugs make news headlines. In the past there was never a need to design a system that could cope with a malicious agent.

We must also consider that what is perhaps the most fundamental feature in the software world—the ability to easily patch and update systems—is a rare commodity in the automotive world. Only 37% of the Ponemon automotive study respondents reported that they support 'over-the-air' updates, and 25% reported that they don't deliver security updates at all.

This means that to update systems and fix security issues, the majority of the auto industry relies on owners to deliver their vehicles to the dealership for maintenance. When vulnerabilities are serious, this procedure is unavoidable and leads to a recall.

Software security is a marathon, not a sprint. Every organisation in every industry faces similar challenges, and we can learn a lot from what others have already achieved. Cybersecurity is a field where having good benchmarks, collaborating with others, and making incremental improvements pays off. Gaining visibility into the process of improvement and having a framework to manage a path to maturity are instrumental in making sure that resources and efforts committed are yielding optimal results.

Organisations like Microsoft and Adobe can release security fixes to customers every week, sometimes even without having to disclose the nature of the security flaw in the system. A car manufacturer, however, is required by law to publicly announce the risk identified and absorb the financial cost of individual car owners bringing their vehicles to a service centre for remediation. This also doesn't consider the legal fallout that often follows.

The consensus among security professionals is that there is no reasonable way to create a system that is 100% protected, 100% of the time. But perhaps we shouldn't define our goal that way. Instead, we should focus on fixing the underlying issues perpetuating the problem.

Here's how to get started:

Embed security

Acquire a skilled development team that stays informed of the risks that unsecured code creates and that infuses secure coding methodologies into every step of vehicle design and production. This is a guaranteed path to a higher quality product with fewer weaknesses and vulnerabilities.

Implement rigid supply chain management

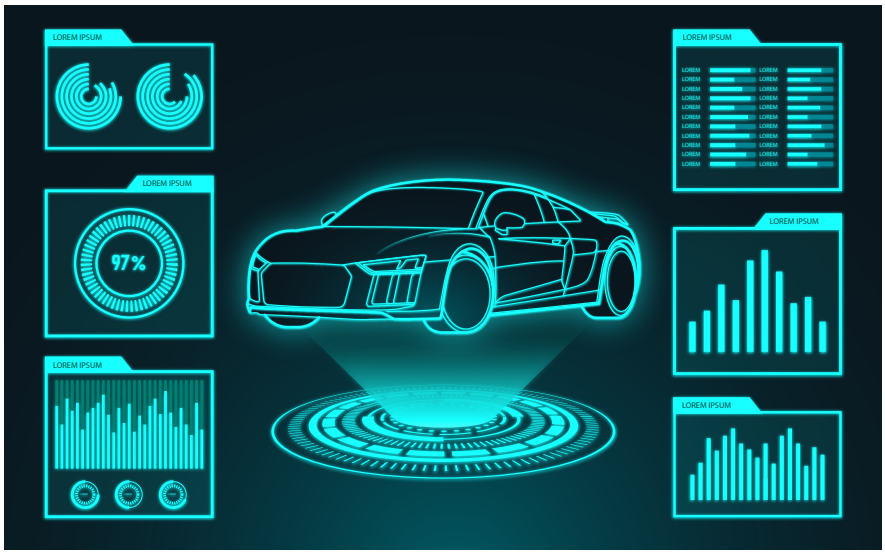
Apply the 'zero-trust' security principle to the supply chain. Enforce strict controls on the use of any third-party code (with an emphasis on open source). Manage an inventory of all software packages in use. Subscribe to a threat intelligence service that provides proactive alerts for newly discovered weaknesses and vulnerabilities.

Create mature security practices

Software security is a marathon, not a sprint. Every organisation in every industry faces similar challenges, and we can learn a lot from what others have already achieved. Cybersecurity is a field where having good benchmarks, collaborating with others and making incremental improvements pays off. Gaining visibility into the process of improvement and having a framework to manage a path to maturity are instrumental in making sure that resources and efforts committed are yielding optimal results.

There isn't a simple step-by-step solution to follow for complete remediation. The strategy to build robust and secure systems has various aspects beyond technical implementation. The three principles listed above are a strong start on your journey to more mature and secure systems.

To achieve the ultimate goal of a smart transportation solution that isn't an easy target for malicious agents, the industry must come together. We must promote knowledge sharing, collaborate in creating the frameworks for guidelines and standards and constantly improve the tools and talent tasked with this responsibility. SST



What Every Security Leader Needs To Know

►► **By Miju Han,** Director of Product Management at HackerOne

As a Director of Security, it's your responsibility to create an environment that encourages greater security.

But how do you create programmes that deliver security at DevOps speeds? How do you stay ahead of coding errors that can cause large amounts of damage? And do you share what you've learned with others or keep it secret?

The Art Of Continuous Security

'Continuous security' may seem like a strange phrase. Nothing is 100% secure. No one silver bullet exists that keeps all systems impenetrable. But that's not the main goal of continuous security.

Continuous security is a defined process that allows you to know what is happening in your environment and react quickly to it. It uses smart automation to make security the default. You make security an intrinsic part of your applications without stopping development teams from delivering quickly.

The use of the term 'art' in the subhead is deliberate. Security in a DevOps environment is often more an art than a science. There are concrete aspects, such as metrics to measure test coverage or policies to prevent

rogue servers or buckets. But how much test coverage is enough? Is it 70%? Or is it 80%? And who should have the authority to create servers - all administrators or just a select few?

These are decisions that have to be made. You can get advice from hundreds of articles on the internet, but the final decision is yours. You make it and you have to live with it.

The best guideline to use is your customers. What will it take to make sure your software is trustworthy? Your goal should be to build software your customers will trust. Often, vanity metrics or minimum thresholds only deliver minimum security. Being trustworthy takes much more than just meeting the minimum.

Build A Culture Of Security

Culture is like the personality of a company. It's the operating environment of a company. It's the values, mission and attitude of a company and its employees.

Security has often been a background process, like scanning for vulnerabilities or performing a vulnerability assessment before deploying to production.

That's not enough for continuous security.

Your developers should understand basic application security principles. They should be trained to understand exactly what processes exist and why. Allow them to spend time with the security team, learning what to look for and what applications look like through the security team's eyes. Allow the security team to spend time with the developers. Learn what security processes get in the way and eliminate them.

Give developers the freedom to experiment. Trust that they want to do the right thing, then verify. When mistakes happen, help solve the problem without placing blame or punishing whoever made the mistake. Instead, fix your systems so the same mistake can't be made again.

'Continuous security' may seem like a strange phrase. Nothing is 100% secure. No one silver bullet exists that keeps all systems impenetrable. But that's not the main goal of continuous security.

Make security worth something. Give $200 to the developer who reports a strange Virtual Machine running in the cloud or fixes a nasty vulnerability without the security team having to ask first. Reward the marketing employee when she reports a phishing email, even when no tests are ongoing.

Build security in as much as possible. Common security features, like authentication and authorisation, should be built into reusable development frameworks. Build servers with automated scripts based on a known secure template. Make security easy. Someone should have to work hard to build an insecure system.

Introduce the entire company to what your security team does and why it's important. Fun events like security expos give you the chance to demonstrate what attackers can do if they succeed in breaching the company. Show a day in the life of a security engineer or incident response engineer. Tell the security team's story, entertain your visitors. If it's memorable, you'll have less friction when you need to introduce new policies or standards.

Above all, make your customer the focus. Build your culture around delivering the best service to your customers — not just keeping the lights on, but becoming trustworthy stewards of their data.

Building a culture takes time, but is well worth the effort. Security has become everyone's job. Make security easy. Make it fun. Make it worth something. SST

Guide To The NTT Security 2019 Global Threat Intelligence Report

For several years, Dimension Data has published an Executive Guide to the NTT Security Global Threat Intelligence Report, providing insights and analysis from its cybersecurity experts about the shifting threat landscape. In its executive guide to the 2019 report, Dimension Data breaks down the report's seven key insights into the cybersecurity landscape.

The NTT Security 2019 Global Threat Intelligence Report offers a high-level overview of the most prevalent threats, motives, and malicious actors observed over the past year, their impact, and recommendations to improve cybersecurity maturity to bolster defences.

1. New dawn rising in the fight against cybercrime

The fightback against cybercrime is gathering momentum, and attracting board-level interest. While the threat landscape will continue to evolve, and the emergence of new, more sophisticated vulnerabilities and attack vectors is inevitable, we should be optimistic about the future of the fight against cybercrime for three key reasons:

- Predictive threat intelligence is reaching new heights.
- Organisations' security investments are becoming more informed, targeted and strategic and cybermaturity benchmarking is gaining popularity.
- There is seeing increasing buy-in and collaboration among stakeholders across the entire cybersecurity value chain.

2. Vulnerabilities surge – and weaponised

During 2018, there was a 12.5% increase in the number of new vulnerabilities discovered. 'Weaponisation' of vulnerabilities is also on the rise. Here, cybercriminals exploit vulnerabilities to launch highly co-ordinated attacks against individuals, businesses and specific groups by using a combination of technical and non-technical tools. Often these vulnerabilities are targeted via automated exploit kits.

Be honest with yourself about your current state of cyber preparedness and vulnerability management capabilities.

During 2018, there was a 12.5% increase in the number of new vulnerabilities discovered. 'Weaponisation' of vulnerabilities is also on the rise. Here, cybercriminals exploit vulnerabilities to launch highly co-ordinated attacks against individuals, businesses, and specific groups by using a combination of technical and non-technical tools. Often these vulnerabilities are targeted via automated exploit kits.

Formulate a plan and roadmap that which is business-led – rather than technology-driven – and identify your immediate priorities to move from your current to your desired state.

3. Cryptojacking rises

Cryptojacking is also is known by several other names, including coin mining, cryptomining, and cryptocurrency mining. In 2018, cryptojacking caught many organisations off-guard and represented a significant amount of hostile activity.

Protect your organisation from the threat of cryptojacking by applying 'least privilege' controls and implementing egress and ingress filtering restrictions, as well as browser plugins to limit site functionality. Also, deny Stratum protocol usage, and segment your network environments.

4. Credential theft: 'handing over the keys to your kingdom'

Credential theft has become increasingly prevalent over the last few years. Credentials are the 'keys to your kingdom' that protect your organisation's networks and data from unauthorised access. This makes stolen credentials a valuable target for threat actors. Phishing and malware are cybercriminals' techniques of choice when it comes to launching credential theft campaigns. And we're seeing a spike in the number of credential theft attacks targeting cloud platforms.

Successfully fending off credential theft attacks on your business involves implementing multi-factor authentication, segmenting your network environment, and enforcing 'least privilege' and segregation of duties. Other recommendations include implementing network activity monitoring and data loss prevention, and educating your employees to be vigilant about phishing attacks.

5. Web-based attacks moving up the stack for profit

There has been an alarming increase in recent cyber attacks in this area. In fact, they doubled year-on-year, (accounting for 32% of all attacks detected during 2018), and represented the top type of hostile activity. Web-based attacks target web-application and application-specific vulnerabilities in technologies frequently used by many businesses. Any organisation that has a web presence is exposed to these attacks and the larger their web presence, the greater the attack surface. Compounding the challenge is that today, more companies' applications are being housed in the cloud which exposes the organisation to new attack types.

Our advice to help protect yourself from web-based attacks includes prioritising patching, segmenting your network environment and enforcing secure coding practices. Also consider deploying application-aware firewalls and performing regular vulnerability scanning.

6. Compliance firmly on the boardroom agenda

Regulatory compliance is a well-known IT risk management challenge faced by many organisations. The General Data Protection Regulation (GDPR) came into effect in Europe in May 2018. Subsequently, a number of other countries have implemented new data protection regulations or are 'beefing up' their existing compliance frameworks and regimes.

Data protection principles and personal privacy rights should put cybersecurity firmly on the boardroom agenda. Ensure that executives understand how cybersecurity and data protection can deliver (or, if ignored, can potentially erode) tangible business value. This will gain their attention and buy-in, and help secure the appropriate investment and drive a top-down focus on changing the behaviours and culture throughout the organisation regarding these issues.

7. Cybersecurity innovations for the future

Today, the ever-evolving threat landscape and increasing compliance requirements and security risks are driving greater levels of cybersecurity innovation. More businesses are seeking to implement emerging solutions to bolster their cyber-resilience.

Keeping an eye on and investing in cybersecurity innovations will ensure that you remain agile and that your business is geared to adapt to the changing threat landscape. SST

Healthcare Breaches Affected Nearly One Million US Patients: The Security Risks of Medical IoT

▸▸ By Check Point Software Technologies Ltd

Over the month of March, nearly one million people in the United States had their medical files exposed in data breaches, according to HIPAA Journal. And after a ransomware attack forced a medical centre in Michigan to close it is evident that healthcare organisations have become an attractive attack target for hackers.

The reason for that is clear: the vast amounts of personal information that hospitals and other healthcare organisations store and transfer electronically. This valuable data can be used to obtain expensive medical services and prescription medications, as well as to fraudulently acquire government health benefits.

The proliferation of IoT medical devices (IoMT) will increase security vulnerability in hospitals and clinics. This means that a new paradigm is required in order to provide full threat prevention to these organisations.

Make no mistake, IoT devices make our lives easier. Organisations across all industries have rapidly adopted them to improve operational efficiency. However, in our recent report into Cloud, Mobile and IoT platforms, IoT devices were recently identified as one of the weakest links in an IT network.

Why is this?

- IoT devices are often built on outdated software and legacy operating systems that leave them vulnerable to attack.
- IoT devices are increasingly collecting and storing vast amounts of data, which makes them an attractive target for cyber criminals.
- IoT devices serve as an easy entry point for attackers

looking to move laterally across an IT network and gain access to more sensitive data. Alternatively, the devices could be attacked directly and shut down.

The healthcare industry is one industry in particular that has moved towards the Internet of Medical Things (IoMT) in a big way. By some estimates, 87% of healthcare organisations will have adopted IoT technologies by the end of 2019 and there will be almost 650 million IoMT devices in use by 2020.

Take ultrasound machines, for example. Ultrasound technology has made huge advancements over recent years to provide patients and doctors alike with detailed and potentially lifesaving information. Unfortunately, though, these advancements have not extended to the IT security environment in which these machines sit, are now connected to and transfer images within.

Check Point Research recently highlighted the dangers this could pose by getting its hands on an ultrasound machine and investigating what takes place under the hood. It discovered the machine's operating system was Windows 2000, a platform that, like most other IoMT devices, no longer receives patches or updates and thus leaves the entire ultrasound machine and the information it captures vulnerable to attack.

Due to old and well-known security gaps in Windows 2000, it was not difficult for our team to exploit one of these vulnerabilities and gain access to the machine's entire database of patient ultrasound images.

The Financial Motivation For Attack

Cyber attacks on hospitals occur on an almost weekly basis. The latest example being that of a ransomware attack on the Melbourne Heart Group which saw the hospital's data scrambled by hackers and held to ransom. Other significant attacks seen last year include Singapore's health service, SingHealth, suffering a massive data breach that saw the Prime Minister's health records stolen followed by 1.4 million patient records stolen from UnityPoint a few weeks later. In addition, May 2017 saw the massively disruptive WannaCry attack that caused 20,000 appointments in the UK's NHS to be cancelled and over £150 million spent on remedying the attack. Interestingly, it was unpatched Windows systems that lead to such damage.

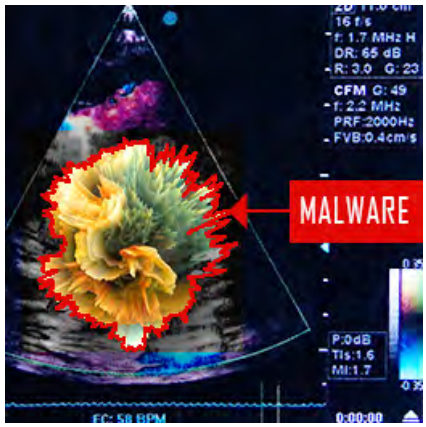


Photo courtesy of Check Point Software Technologies Ltd

However, it is primarily not mass disruption that motivates cyber criminals to target the healthcare industry. Due to the vast amounts of personal information that hospitals and other healthcare organisations store and transfer electronically, these institutions make for attractive targets to attack. This valuable data can be used to obtain expensive medical services and prescription medications, as well as to fraudulently acquire government health benefits. It is no wonder then that this information can fetch as high as US$60 per record on the Dark Web.

Although there are many articles describing the personal danger of cyber attacks to patients, the financial damage is far more realistic and is what lies at the heart of cyber attacks on the healthcare industry.

According to the Ponemon's Cost of Data Breach Study, at US$408 per health record, the healthcare sector has to foot the highest cost by far to remedy a data breach. This stands in contrast to the average of US$225 per record paid by other organisations. These costs include fees to investigate and repair the damage caused by an attack as well as paying fines or ransoms or any stolen funds themselves. Attacks can also result in a loss of patient records and information as well as cause long-lasting damage to the health institution's reputation.

The Security Problem

The risk of a cyber attack on healthcare organisations is huge. Such attacks could lead to loss and sharing of personal data, altering a patient's medical information regarding medicine, dosages and more and hacking of MRI, ultrasound and x-ray machines in hospitals.

The critical nature of healthcare environments also means that many of those involved in the healthcare process often require immediate access to patients' data across a large range of devices and applications. As a result, downtime to update or patch systems is not an option that is easily afforded. In addition, this large range of medical devices from many different manufacturers makes for an IT security manager's nightmare. He has to not only monitor them but also integrate a security policy that incorporates them all.

From the hospital management's perspective, downtime to update or patch systems not only affects the operational flow of the hospital itself but can also hit the financial bottom line too. Having spent very large amounts on important healthcare equipment, it is vital that management sees a return on its investment by having that equipment up and running in order to be able to cover their costs through claims from patients' medical insurance policies.

From a regulatory point of view, the inherent vulnerabilities that come with operating healthcare devices, such as a lack of encryption of sensitive data as well as hard-coded or default login credentials, prevent IT professionals from even implementing security patches, should such patches even exist.

The Secure Solution

The abovementioned security vulnerabilities highlight the importance healthcare organisations must place on their IT security posture. While there are still issues and vagueness when it comes to security protocol standardisation across Internet of Medical Things (IoMT) devices, there is still much that healthcare organisations can do to protect their patients' data.

Photo courtesy of Check Point Software Technologies Ltd

Healthcare organisations must remain alert to the multiple entry points that exist across their network. There can often be hundreds, if not thousands, of devices connected to the IT network, any one of which contains security vulnerabilities in either the hardware or software used by such devices. Catching every one of these vulnerabilities is impossible however, so it is essential healthcare organisations have an advanced prevention security solution in place to catch the inevitable attacks that will attempt to exploit these vulnerabilities.

In addition, segmentation can never be overstated. Separating patient data from the rest of the IT network gives healthcare IT professionals a clearer view of network traffic to detect unusual activities that might indicate a breach or compromised IoMT device. Segmentation would also enable these organisations to prevent data stealing or encrypting malware from propagating further across the network and to isolate the threat.

Finally, segmentation should also apply to healthcare personnel within the organisation with access to those systems provided only to those who actually require the access to carry out their roles.

Conclusion And Takeaways

The benefits that connected medical devices offer cannot be ignored. They provide patients and healthcare providers with potentially life-saving information and enable an efficient way of handling this information. However, healthcare organisations must be aware of the vulnerabilities that come with these devices that increase their chances of a data breach. Network segmentation is a best practice that allows IT professionals in the healthcare sector the confidence to embrace new digital medical solutions while providing another layer of security to network and data protection, without compromising performance or reliability.

Once best practice cyber hygiene is implemented and enforced, IT security teams can rest assured their patients' records and, in turn, their organisation's finances and reputation, are safe. SST

ASEAN Managed Security Services Market To Grow Significantly

Rapid rise in demand for managed security services among ASEAN countries (a group of 10 countries in Southeast Asia) will see the ASEAN managed security services market grow by 18.6% on a year-over-year basis, according to market research firm Research and Markets.

The managed security services segment is set to maintain a strong growth momentum from 2017 to 2022.

Monitoring/management services remained the largest revenue contributors to the market, generating more than 75% of the overall market value as businesses in ASEAN continued to prefer traditional managed security services, be it system health check, security asset monitoring/management, compliance and other perimeter security monitoring/management services.

Geography wise, the market was dominated by Singapore, Malaysia and Thailand, with Singapore contributing to more than 60% of overall ASEAN market revenue. There are several factors driving the strong adoption of managed security services in Singapore. Key factors include higher awareness of cybersecurity, a stronger managed security services ecosystem, stronger demand for advanced threat management, stricter compliance requirements and cost management.

Malaysia remained the second largest adopter of managed security services in 2017, making up 12.4% of the ASEAN market share. Businesses in Malaysia tend to stick to basic managed security services. The drop in market growth over the last one to two years was mainly due to an insourcing trend among banks and large insurance companies, the largest adopters of managed security services in the country.

Banking, financial services and insurance (BFSI) and government verticals remained the top two spenders of managed security services in 2017. Increasing adoption was also observed in other verticals such as manufacturing and education.

However, even as organisations in ASEAN increase their investment in security measures for better security protection and risk management, they face growing challenges in security operations, with a shortage of professionals and domain expertise leaving them vulnerable to data breaches and other security threats.

The recent data breaches of more than 46 million mobile users' personal information in October 2017, and the data breach of SingHealth in Singapore are typical examples of threats that organisations encounter that may have resulted from a shortage of security professionals. SST

Turning Data Into Disruption: The Story Of 2019

►► **By Brian Householder,** Chief Executive Officer of Hitachi Vantara

Disruptive businesses are always looking forward to the road that lays ahead and, in this instance, for me, in 2019, the theme that will permeate this year and beyond is change.

The business world is quite familiar with change. From the industrial revolution where water and steam became power to mechanise production, all the way to the birth of the internet and beyond: It's always present. So why is 2019 different? Here are four reasons that I believe it is.

1. Exponential Change Has Become The New Normal
As I stated above, none of us is a stranger to change. But what we are beginning to see now and what we will see much more of this year, is a new rate of change, one that will eclipse anything that's come before. What's driving it all is data and this data mountain is growing. According to MicroStrategy, by 2025 the global datasphere will grow to 163 zettabytes, 10 times the amount of data generated in 2016.

Today businesses have access to more data than ever and for companies that play their cards right, it can completely change the game. In 2019 we will see a growing number of disruptive-minded businesses doing just that by:

- Reimagining every single part of their business, including how they transform, the solutions and services they provide, how they can operate differently and more.

- Changing expectations that will impact all of us, whether you are CEO, CIO or CMO, a big business or a small business. For example, rather than serving as the custodian of technology assets in a business, CIOs will change their role to focus on applying technology and company data and figuring out how they can harness it to drive digital transformations.

According to Dennis O'Brien, chairman of Digicel's World Economic Forum, "We're poised to experience more digital

This year, the disruptive organisations will look for orchestration capabilities that streamline the machine learning workflow. In doing so they will help data scientists, engineers and analysts collaboratively build and deploy predictive models from big data that they can then use to fuel their business transformation.

progress in the next 10 years than we have in the last 50." This progress will really begin to shine in 2019 when more businesses choose the transformation route, becoming disrupters that harness one of their greatest assets, their data, using new innovative technologies. These companies will secure insights that can advance the business while helping them keep the unique needs of each customer at the centre of everything they do.

2. AI And Machine Learning Become Mainstream
When we talk about activating our data and changing the game, the discussions often revolve around innovations such as AI and machine learning. In fact, we've been hearing about these innovations for so long, there's a pervasive feeling that they're already meeting their promise. This mindset is premature. It's true that AI and machine learning have advanced significantly and continue to evolve, especially as more data becomes available but here's the challenge: Data scientists are still spending too much time finding, cleaning and reorganising huge amounts of data rather than analysing it.

This year, the disruptive organisations will look for orchestration capabilities that streamline the machine learning workflow. In doing so they will help data scientists, engineers and analysts collaboratively build and deploy predictive models from big data that they can then use to fuel their business transformation.

Winning solutions will enable smooth team collaboration, maximising limited data scientist resources and putting predictive models to work on big data faster, regardless of use case, industry or language. Does this sound familiar? It should. Last year we introduced these capabilities in Pentaho, which streamlines the entire machine-learning workflow. It's through solutions such as this that the 80/20 rule of data scientist productivity will be a thing of the past.

3. The Disrupters Assume A Commanding Lead
When we talk about exponential change, it's inevitable that some businesses will have success while others don't. GoodData CEO Roman Stanek summed it up nicely in a Forbes article where he said, "embracing disruption is easier for some companies than it is for others".

There are many reasons why a business will become a laggard. It could be due to leaders not buying into this new mindset or a small business not having the resources needed to transform. Whatever the reason, a very clear gap will develop in 2019 that separates the disrupters from the disrupted. Imagine the Jamaican sprinter Usain Bolt and the separation he creates in a 100-metre race. That's the type of performance gap I am talking about.

There is some good news for those who are late to the race. Unlike an Olympic sprint, there is no finish line in the business world, which means that lagging companies can get back into the race. Just keep in mind that the longer you wait, the harder it will become to be relevant.

4. Exponential Changes Take Employees Back To The Classroom
Education is something I could have touched on above but I think it warrants its own time in the spotlight because, in my eyes, there's a somewhat frightening trend taking place — today the rate of industry change equals or exceeds the rate of learning within a given business. If that thought isn't daunting enough, consider this: The lifespan of many skills we learn is shrinking due to the rapid pace of innovation around the world.

Here's just one example. According to GitHub, "Software engineers must now redevelop skills every 12 to 18 months." Just think about that for a moment. A person you hire today who has mastered a critical skill could be obsolete in less than two years if they don't evolve. That's why exponential learning programmes are vital.

Over the course of the next six months companies with the disrupter mentality will follow this same path, shifting greater resources to the ongoing education of their most valued asset, their employees. The goal of these efforts will be to provide each person with the insights and skills needed to stay a few steps ahead of the changes lurking around each corner of the industry.

If 2018 and the first half of 2019 taught us anything, it's that the pace of innovation has ascended to unimaginable levels. Over the course of this year, we will see a growing number of companies that are thinking differently, planning differently and ultimately acting differently by taking the disruptive approach to their business. These are just four areas where I think this shift will be most visible. SST

From Fortress To Airport Security: Understanding The Shifting Cybersecurity Paradigm

►► **By Miju Han,** Director of Product Management at HackerOne

There has been a dramatic shift away from the traditional cybersecurity 'fortress' strategy to a new, modern approach that understands that there is no way to be 100% secure.

Building a fortress has been the typical security model for years, where firewalls are expected to protect assets from outsiders and a limited number of entry points enable the tracking of data flow and access. Once inside, however, users have free access (because, presumably, they've been vetted). It essentially relies upon one hardened entry point that, if overcome, leaves everything of value unprotected.

This is no longer safe because criminals have figured out how to get over these walls with social engineering, malware and other tactics. Plus, humans tend to make mistakes and leave a known or unknown door open by placing data on a public server or failing to patch a technology gap.

Today, it's clear this fortress approach has become insufficient on almost every front.

The New Approach - The Airport Model

The new approach to cybersecurity is analogous to how an airport approaches security, with many layers of vetting, many different types of security and many different areas requiring different credentials to access.

In an airport, anyone can walk into the ticketing area. But to get past the first security point, your documents are closely checked, then you and your bags pass through machines that scan for liquids, flammables and weapons. Then, getting on the airplane requires a barcode scan of your boarding pass, getting on the tarmac requires a badge and a door access code, and so on. This multi-layered approach to security uses varying safeguards as travellers and workers move between areas requiring more or different security.

For cybersecurity, that's akin to multiple levels of firewalls and passwords, two-factor authentication, biometrics, logging and surveillance to alerts to odd activity, additional focus on critical assets and more. This strategy, termed 'defence in depth', relies on continuous and ever-more stringent access and technological controls.

Focus On Managing Probabilistic Risk, Not Eliminating It

There is no way to achieve complete security. With the world becoming more connected and data becoming more centralised, the need for access will only increase. That means companies need to focus its limited resources based on the highest risk.

First, however, security leaders need to understand which risks are greatest and which of those are most likely. Probabilistic risk management or assessment is the process of identifying a specific problem, gauging the possible damage from it and estimating the likelihood of it happening. From there, they can prioritise where to focus their efforts.

Security From The Developer's Point Of View

Security cannot happen without the developers being on board. The relationship between the security and development teams is foundational to good security.

It's important for development teams to understand that the security teams are there to help them find solutions. Security teams aren't the 'code cops' coming to break down their door. They are not trying to get in the way of delivering functionality. Instead, security leaders are helping them to find solutions to fundamental security problems. They should be working together, with an equal say on both sides, to create solutions that please both sides.

Security From A User's Standpoint

An important piece of a sound security foundation is the viewpoint of the end user. Some products are used by employees, others by paying customers. Both viewpoints are key to a successful security strategy.

Good hackers get familiar with the product and try to put themselves in the role of a user. They try to break the system by doing unexpected things. They ask themselves: "What can a user do to make the system do something it shouldn't?"

Security leaders should be doing the same. Start by walking through the employee on-boarding process from start to finish. Pay attention to the processes used to create accounts, provision hardware and create passwords. Don't search for vulnerabilities but pay attention to inefficiencies or glaring problem areas.

After an internal look, walk through a customer's experience in buying your product. Start with marketing and move through account access, entering credit card information or however a particular flow takes an end user from product awareness to paying customer.

Understanding these flows can better inform your company's strategy moving forward. The security team would be able to view the systems through the eyes of the end user.

Good hackers get familiar with the product and try to put themselves in the role of a user. They try to break the system by doing unexpected things. They ask themselves: "What can a user do to make the system do something it shouldn't?"

Understanding Threats Against Your Systems

Threat modelling is the practice of reviewing the design of a system to find threats against that system. These threats are recorded and mitigated to the extent possible.

Threat modelling allows the security teams to anticipate problems. Use it to identify threats against your systems and possible weaknesses attackers could exploit. When done early enough in the development life cycle, major problems are fixed before they can be exploited.

The goal now is to manage risk as best as possible, to be transparent on vulnerabilities and collaborate with others on solutions and tactics, and to be open (and thankful) to anyone who points out a potential security gap.

Today, organisations are more open to learn from every security experience, to share with others, and to correlate actions with results. This openness is reflected in the huge number of industry groups and government agencies promoting vulnerability disclosure policies as a best practice. It's also apparent in the increasing prevalence of legislation and regulation covering data privacy, access and disclosure. Setting a secure foundation helps companies remain stable as security teams implement appropriate security strategies. SST

Keeping Our Smart Buildings Safe

►► **Ken Lim,** General Manager and Managing Director, Building Technologies and Solutions, Singapore at Johnson Controls

Smart buildings are on the rise. Powered by integrated building management technology at its core, a smart building is more energy efficient and keeps its occupants safe and comfortable. Gone are the simple mechanical, pneumatic and electrical controls that regulate the ambient environment. In their place is a complex building automation system (BAS) that integrates various monitoring and control solutions such as heating, ventilation and air-conditioning (HVAC), lighting, fire, security and networking onto a single platform.

Buildings are the next big frontier for Internet of Things (IoT) and data. A smart building uses data generated by IoT-enabled equipment, coupled with data gleaned from external sources, to allow for performance-enhancing, energy-saving decision making.

The Asia Pacific region is the largest spender on IoT, according to analyst Frost & Sullivan. The total spending on IoT in the region is expected to reach US$59 billion by 2020, a big jump from US$10 billion spent in 2014.

South Korea and Singapore are likely to be among the top five countries globally to adopt IoT.

However, what makes a building 'smart' is also what makes it vulnerable to cyber attacks. Most IoT devices such as smart meters, though not designed for web browsing, are connected to the Internet for control and analytics purposes. Without stringent security controls in place, these devices can quickly be targeted as areas of entry by hackers. Compounding the issue is the lack of global security standards to govern the plethora of IoT devices available. Similarly, poorly secured wi-fi servers could be exploited.

Damages from cybersecurity breaches can be far-reaching. The average cost estimate of a cyber intrusion exceeds US$1 million, together with significant impact on brand reputation, stock prices and productivity.

Securing smart buildings requires a blended approach of risk-based planning, security architecture, technology, processes and people skills. Such rigour - a commonplace practice in IT systems - is not typical of BAS. Given the evolving threat landscape, it's time that the strategy of protecting smart buildings keeps apace with changing times.

The Human Factor

Cybersecurity is everyone's responsibility, from building occupants to facilities managers. It's imprudent to take a 'don't-worry-nobody-will-know' or 'it-doesn't-matter' attitude when it comes to matters of cybersecurity.

For individuals, knowing what behaviours will lead to a more or less secure network, coupled with up-to-date awareness of emerging threats, are basic cybersecurity awareness. Having strong passwords and sound password management are also good practices that help thwart hacking attempts.

Organisations need more stringent cyber controls. They could consider implementing two-factor authentication to employees who access systems where the most sensitive or confidential data (for example, patient database) are stored. Regular security audits to validate security measures would also help to prevent complacency.

Buildings are the next big frontier for Internet of Things (IoT) and data. A smart building uses data generated by IoT-enabled equipment, coupled with data gleaned from external sources, to allow for performance-enhancing, energy-saving decision making.

Protecting The Building Automation Systems

Securing the smart built environment means focussing on what must be protected and how to prevent intruder access. The integrated BAS can be vulnerable to intrusions from within a corporate network. For instance a hacker could gain access to the HVAC controls to compromise the stable environment within a laboratory thereby destroying years of research.

Ransomware attacks BAS the same way as it does other embedded controls systems. The BAS can be crippled through attacks on the operating system of the server, or by making critical files such as configuration and database files inaccessible.

It is good practice to deploy the BAS on a private network and to protect it from the Internet by a firewall. The servers should neither be used to check email, nor used to access websites that are not required for the running and management of the BAS. It's also important to keep the systems updated with the latest anti-virus software, revisions and patches as well as conduct regular backups.

All building data needs to be encrypted at rest and in transit using industry-leading protocols. The platform itself should be protected by a regulated access control system and data masked to restrict access to sensitive information.

Know Thy Devices

A robust endpoint security strategy in smart buildings is essential. The sheer number and variety of endpoints — mobile phones, tablets and printers for instance — could be targeted for unauthorised access. Email phishing and malware are usually distributed through the Internet; hence any end device that accesses the web and receives email attachments carries a degree of security risk.

Retaining control of systems and devices is just as crucial. It is important to identify and authenticate all devices and machines connected to the network. This would mitigate the risk of a hacker inserting a rogue, untrusted device into the network and taking control of any systems or machines. Strong cybersecurity solutions such as advance detection traps or stroke count traps recognise any forms of unknown actions and lock down or isolate the network immediately to prevent any further damages.

Cyber-Physical Security

A converged cyber-physical security application can bolster the overall security of smart buildings. This strategy relies on Artificial Intelligence (AI) to address real-time threats, while keeping a check on false alarms.

The analytics platform connects and combines data from internal and external sources with advanced risk algorithms to provide proactive threat protection.

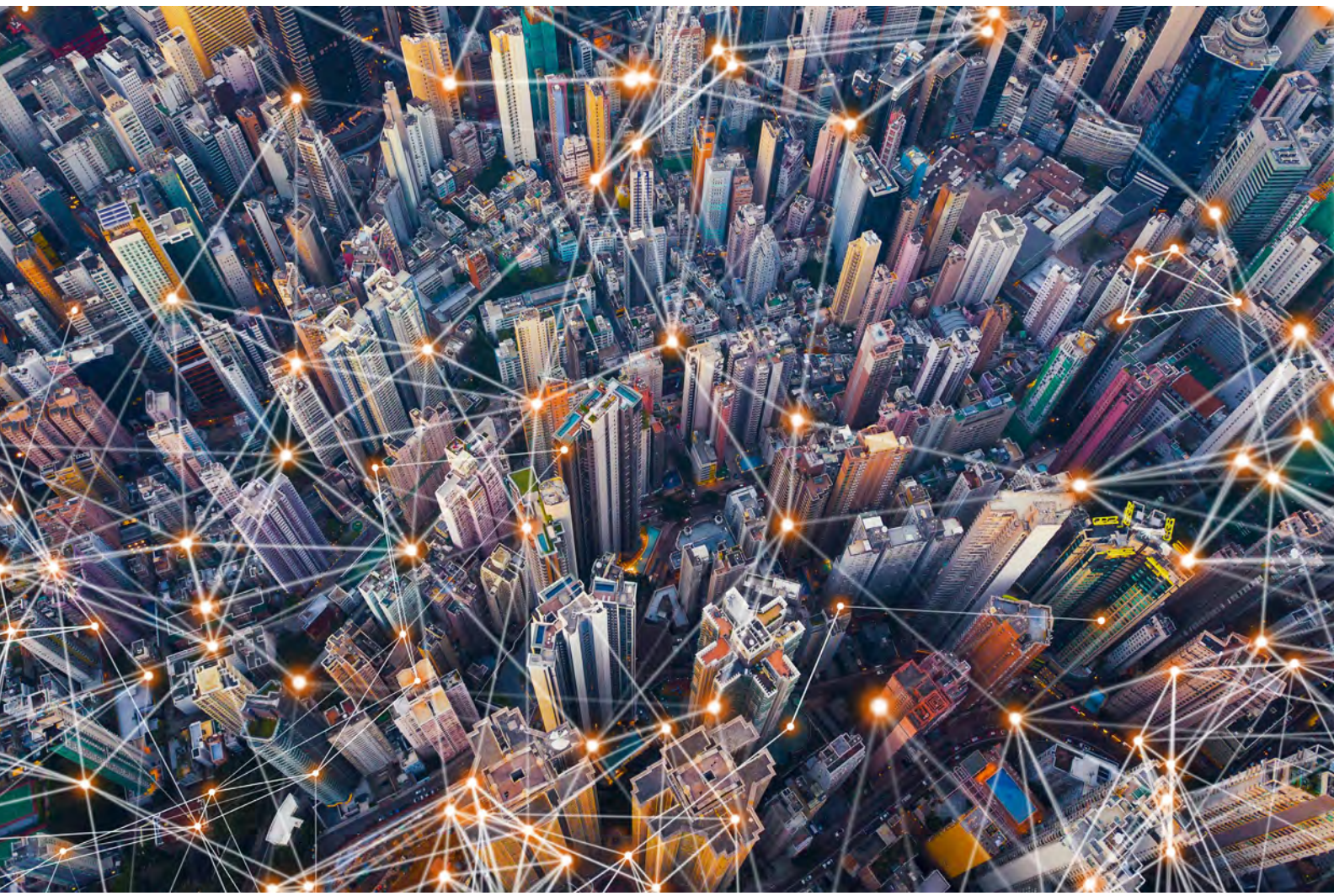
By decreasing alarm 'noise', the approach allows security teams to focus attention on the highest priority events. Through this process, information is put into context and ranked by risk severity — all this provides a complete security picture, enabling the deployment of the right security resources on the right security priorities.

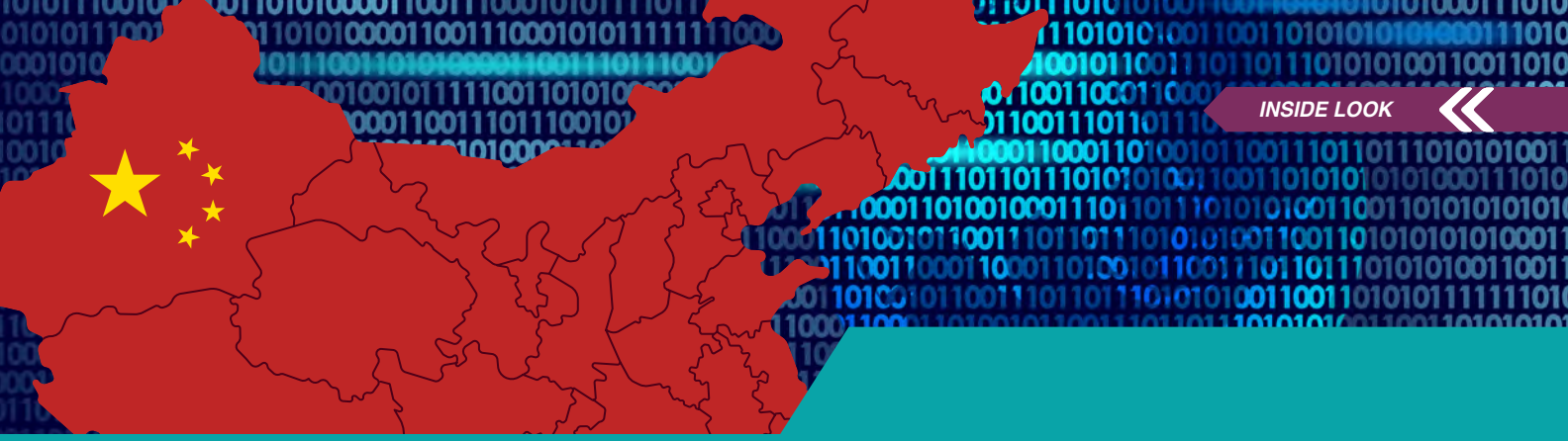
The Collaborative Factor

Today, the role of a facilities manager goes beyond running a building. With the BAS technology now containing more IT-based hardware and software, facilities managers should collaborate with IT experts to address any cybersecurity concerns that threaten the smart built environment and, by extension, the building's occupants. No two smart buildings are exactly alike. The right systems integrator takes a holistic view of the building's systems, then designs and installs technology to support the business objectives for the building, delivering better outcomes for the occupants. The right BAS is optimised for the building to operate more efficiently and sustainably while improving comfort and safety.

It's hard for one organisation to go it alone in battling the rapid evolution of cyber threats. Industry initiatives such as the ISASecure, which industrial systems manufacturer Johnson Controls is a strategic member of, are setting international cybersecurity standards and certification for the global ecosystem of intelligent buildings and smart city technologies.

In summary, securing smart buildings and building systems is a shared responsibility requiring focus and commitment from multiple parties. Businesses and organisations would benefit from a streamlined, multi-pronged approach that protects data, devices and manage security incidents, as well the continual improvement of risk management for better overall operational efficiency. SST





Greater China Managed Security Services Market To Grow Robustly To 2022

The Greater China Region Managed Security Services market will grow at a lively pace from now to 2022, according to a report by Research And Markets.

The market research firm reported that the Greater China MSS market maintained its double-digit growth of 18.3% on a year-on-year basis in 2017.

This strong growth is due to the introduction of new cybersecurity laws and guidelines from local authorities. Stricter compliance put enterprises under greater pressure to meet specific requirements leading to an increase in enterprises looking for third-party experts to manage their security for improved cyber resilience.

In addition, the evolving sophistication and complexity of the threat landscape - be it high-profile volumetric DDoS attacks, ransomware attacks, data exfiltration or cyber extortion - and the increased media coverage of these high-profile cyber attacks, drove enterprises to review their cybersecurity strategy.

The Greater China market is expected to witness a healthy compound annual growth rate over the next five years, as enterprises move beyond cyber responsiveness to cyber resilience.

At the country level, China led in the adoption of managed security services in the Greater China region, followed by Hong Kong and Taiwan. With more enterprises in China recognising the value of managed security services, the market experienced the strongest growth among the countries in the region in 2017.

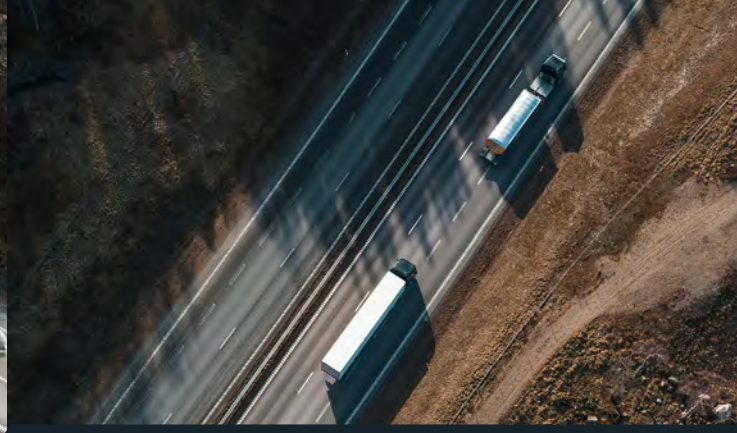
Within China, banking, financial services and insurance, government, and service providers were the larger spenders on managed security services in 2017.

Consumer premise equipment-based (CPE) services continue to dominate the total managed security services market with a market share of more than 70% by 2022. This segment is expected to grow faster than the hosted segment. Hosted Security as a Service is expected to grow at a compound annual growth rate of 22.1% from 2017 to 2022. The segment grew at a slower pace than the CPE-based segment as large enterprises were either restricted by local regulatory requirements or prefer to engage managed security services providers to supplement their in-house security team.

In terms of revenue, Hong Kong remained the second largest managed security services market in the region. The Hosted Security as a Service segment is expected to grow at a faster pace than CPE-based segment in Hong Kong. As for verticals, banking, financial services and insurance and government continued to be the largest revenue contributor of managed security services in Hong Kong.

The adoption of managed security services in Taiwan remained the lowest in the region. Banking, financial services and insurance, government and manufacturing verticals continued to be key managed security services spenders in 2017. The education vertical was the fastest growing vertical due to concerns over protecting valuable proprietary research data that is increasingly targeted by cybercriminals.

Research And Markets projects that enterprises in the region will gradually shift to a more proactive security approach and move beyond traditional reactive perimeter defence mode. SST



Distance Alert From Volvo Trucks Helps Drivers Keep Safe Distance

Volvo Trucks has introduced a new safety function, Distance Alert, that makes it easier for truck drivers to keep a safer distance from the vehicle ahead and avoid critical situations. Accidents where one vehicle runs into the back of another currently make up around 20% of all serious collisions involving trucks.

Often accidents of this kind are caused by inattention and trucks keeping too close a distance from the vehicle in front. Distance Alert warns drivers with a red light in the windscreen as soon as the truck gets too close to the vehicle ahead and in most cases a collision can be prevented, said Carl Johan Almqvist, Traffic and Product Safety Director at Volvo Trucks.

When Distance Alert detects that vehicles are closer together than the selected time gap of 1.5 to 3.5 seconds, a red light appears in the windscreen. If the driver does not slow down, the collision warning system is activated and emits audible and visual signals of increasing intensity. This involves a flashing light and an audible alarm. Finally, the advanced emergency brake is activated. All of this happens within just a few seconds.

The new function is intended for use on major roads outside cities and is switched on at speeds over 60 km/h, unless the adaptive cruise control system is in use. In the same way as the collision warning system's other functions, Distance Alert uses a combination of camera and radar technology to calculate the distance and identify objects on the road.

"For haulage companies, investing in safety makes sense not only to protect people, but also to save money. Lower insurance and repair costs and less unplanned downtime are some of the arguments. In addition, a safe driving style is generally fuel-efficient. The combination of well-trained, safety-conscious drivers and safer trucks benefits everyone," said Almqvist. SST

Delta Barricade Prevents 2 Vehicle Attacks At US Naval Station

On June 3 2019, when a man couldn't produce credentials at Mayport Naval Station, he gunned his engine and attempted to enter. The security staff activated their vehicle access barrier, a Delta DSC501, to pop out of the ground. The vehicle crashed into it and was brought to a standstill. The violator was taken to the hospital and died two days later.

Eight days later, another man driving a Ford F-350 truck also tried to get on base. Once again, the DSC501 popped out of the ground and the attacker collided with it, stopping the truck in its tracks. The violator was arrested and is now facing state and federal charges.

The high security barricade is supplied by Delta Scientific, a manufacturer of counter-terrorist vehicle control systems. Originally designed for the U.S. Navy, the anti-terrorist barrier has also been selected for use at U.S. embassies. Set in a foundation only 18 inches deep, the Delta DSC501 is able to survive and operate after a 1.2 million foot pound impact.

In testing, the DSC501 not only stopped and destroyed a 65,000-pound dump truck but the barricade continued to stand, preventing a potential second attack.

The Delta DSC501's K12/L3 certification meets the government's highest requirements. With its shallow foundation and aesthetic design, it does not get in the way of buried pipes, power lines and fiber optic communication lines. The shallow foundation also reduces installation complexity, time, materials and corresponding costs. SST

Canada–Netherlands Biometric Programme For Paperless Cross-Border Travel

In June, an agreement was signed on the Known Traveler Digital Identity programme, which will facilitate paperless border clearance between Canada and The Netherlands.

The programme will allow travellers flying between the two countries to enjoy a seamless journey, where a simple face scan will be enough to identify the passengers boarding a plane at departure and to clear immigration on arrival. They won't need to show their travel documents or go through any further checks.

The agreement to design and implement the Known Traveler Digital Identity Pilot Project was signed by The World Economic Forum and the governments of Canada and The Netherlands, in collaboration with implementing partners Air Canada, KLM Royal Dutch Airlines, Amsterdam Airport Schiphol, Toronto Pearson International Airport and Montréal-Trudeau International Airport, and technology partners Accenture and Vision-Box.

The pilot will be based on the issuance of a digital identity – a Passenger Data Envelope – for each passenger prior to departure, including the self-service enrolment of their biometrics via a dedicated application. The identity is authenticated by the participating government. This authentication then virtually travels between the two countries, pre-approving the passenger to clear the border on arrival as a 'Known Traveler' without needing any checks aside from a quick face scan on the move. This is made possible because the destination authority has been provided with early, trusted and verified information prior to the passenger's arrival.

This actionable intelligence at the arrival is facilitated by the Vision-Box Orchestra platform already deployed at Schiphol Amsterdam, as part of its Seamless Flow programme which allows automated border control to operate in contactless mode.

The Known Traveler Digital Identity is an example of enhanced intergovernmental and public-private cooperation realised under a unique interoperable framework of digital identity. By connecting the departure with the arrival of a passenger, the journey is substantially streamlined, avoiding repeated tasks, improving the safety of citizens and optimising operations.

This offers proof that the public-private collaboration where governments act as trusted identity brokers is expected to become a fundamental pillar of end-to-end seamless travel.

It is an important step in the usage of leading-edge technologies at the service of the cross-border movement of people, said Vision-Box CEO Miguel Leitmann.

"It will contribute to the establishment of standards for global interoperability and privacy-preserving identity management models that will bring significant opportunities for the aviation, travel and tourism industries."

A demo of this concept was conducted in Montreal at the agreement signing event. SST

A Great Leap Forward In Human-Machine Interface?

Ultra-small nanoprobes could be a leap forward in high-resolution human-machine interfaces. Machine enhanced humans – or cyborgs as they are known in science fiction – could be one step closer to becoming a reality, thanks to new research from the University of Surrey and Harvard University.

Researchers have conquered the monumental task of manufacturing scalable nanoprobe arrays small enough to record the inner workings of human cardiac cells and primary neurons.

The ability to read electrical activities from cells is the foundation of many biomedical procedures, such as brain activity mapping and neural prosthetics. Developing new tools for intracellular electrophysiology (the electric current running within cells) that push the limits of what is physically possible (spatiotemporal resolution) while reducing invasiveness could provide a deeper understanding of electrogenic cells and their networks in tissues, as well as new directions for human-machine interfaces.

In a paper published in Nature Nanotechnology, scientists from Surrey's Advanced Technology Institute (ATI) and Harvard University detail how they produced an array of the ultra-small U-shaped nanowire field-effect transistor probes for intracellular recording. This incredibly small structure was used to record, with great clarity, the inner activity of primary neurons and other electrogenic cells, and the device has the capacity for multi-channel recordings.

Dr. Yunlong Zhao from the ATI at the University of Surrey said, "If our medical professionals are to continue to understand our physical condition better and help us live longer, it is important that we continue to push the boundaries of modern science in order to give them the best possible tools to do their jobs. For this to be possible, an intersection between humans and machines is inevitable."

"If our medical professionals are to continue to understand our physical condition better and help us live longer, it is important that we continue to push the boundaries of modern science in order to give them the best possible tools to do their jobs. For this to be possible, an intersection between humans and machines is inevitable."

- Dr. Yunlong Zhao, ATI at the University of Surrey

"Our ultra-small, flexible, nanowire probes could be a very powerful tool as they can measure intracellular signals with amplitudes comparable with those measured with patch clamp techniques; with the advantage of the device being scalable, it causes less discomfort and no fatal damage to the cell. Through this work, we found clear evidence of how both size and curvature affect device internalisation and intracellular recording signal."

Professor Charles Lieber from the Department of Chemistry and Chemical Biology at Harvard University said, "This work represents a major step towards tackling the general problem of integrating 'synthesised' nanoscale building blocks into chip and wafer scale arrays, and thereby allowing us to address the long-standing challenge of scalable intracellular recording.

"In the longer term, we see these probe developments adding to our capabilities that ultimately drive advanced high-resolution brain-machine interfaces and perhaps eventually bringing cyborgs to reality." SST

Check Point And Microsoft Unite To Help Organisations Stamp Out Data Leaks And Losses

Check Point Software Technologies Ltd, a global provider of cybersecurity solutions, will be integrating Check Point security appliances and the Check Point R80 SmartConsole security management console with Microsoft Azure Information Protection (AIP) to help organisations prevent damaging losses and leaks of sensitive business data.

The integration of Check Point's advanced policy enforcement capabilities with Microsoft AIP's file classification and protection features enables enterprises to keep their business data and IP secure, irrespective of how it is shared. It prevents organisations' employees from accidently sending sensitive business data outside of the corporate network by Microsoft Outlook and Exchange, and extends complete data leak protection capabilities to popular web services such as Gmail, Dropbox, FTP and Box.

When users create or handle files with sensitive data, Microsoft AIP recognises the sensitive nature of the file and prompts the user to label the document as 'Confidential Financial Data'. With this label, no user in the organisation can accidentally send this file to an external recipient or location outside of the corporate network, as the integration with Check Point will block any improper distribution and notify the user. This educates users about correct data handing, helping to prevent future incidents. Microsoft AIP's sensitivity labels can also be applied automatically to documents and files based on the IT administrator's rules and conditions, enabling policy-based detection and protection of sensitive files by Check Point gateways and the R80 SmartConsole management console.

According to the 2019 Verizon Data Breach Investigations Report, 35% of the close to 42,000 breaches analysed occurred as a result of human error. The integration between Check Point's solutions and Microsoft AIP stops these accidental breaches from occurring. It also enables organisations' security and IT teams to track and control the exposure of sensitive information, and to take corrective measures to prevent data leakage or misuse. This gives Check Point and Microsoft customers a truly comprehensive Data Leak Prevention solution that consistently enforces relevant data governance actions no matter where data is stored or who it is shared with.

"User error is one of the leading causes of data breaches, exposing organisations to reputational damage and to penalties from data watchdogs for breaching compliance regimes. Enterprises need a way to protect their sensitive data against accidental breaches, without compromising individual and corporate productivity," said a Check Point spokeperson. "The integration between Check Point and Microsoft AIP robustly protects corporate data against breaches across email, web and FTP services, and gives IT and security teams the tools they need to track sensitive data across networks and rapidly remediate any incidents."

Because the integration between Microsoft AIP and Check Point enables policy-based enforcement of data in transit at the network level, IT and security teams can track and control how documents are being shared and immediately take corrective measures to prevent data leakage. SST

Smart Door Locks Market On A Growth Trajectory In India

The adoption of smart security systems and rising demand for home automation systems for better security in houses will accelerate the growth of the smart door locks market in India in the next few years.

Between 2019 and 2025, demand of smart door locks in the residential and corporate sector is expected to rise at a compound annual growth rate (CAGR) of 35.6%, according to a report by ResearchAndMarkets.

The growing prevalence of IoT in India combined with the increasing number of smart homes are factors behind the growth in the market in India.

At present only a small segment of the Indian population is using smart door locks because of the higher cost of smart door locks compared to conventional door locks. However, rising personal disposable income, surging crime rates and the growing pool of tech savvy Indian consumers would see the demand for smart door lock soar in the near future. This projected increase in Indian consumers using the smart door lock over the next decade would create opportunities for both existing and new entrants in the market.

In 2017, non-mobile app-based smart door locks dominated the market; mobile app-based smart locks accounted for only 14.85% of the total smart door lock market. The remaining 85.15% were for non-mobile app-based (keypad-based) smart door locks. An increase in the number of commercial building in the country contributes to the increase in non-mobile app-based smart door lock growth.

Between 2019 and 2025, demand of smart door locks in the residential and corporate sector is expected to rise at a compound annual growth rate (CAGR) of 35.6%, according to a report by ResearchAndMarkets.

However, with a rising tech-savvy population (especially in metro cities), the mobile app-based smart door lock market will reach US$216.61 million in 2025, up from US$ 15.44 million in 2017 at a growth rate of 39.79%, projected ResearchAndMarkets. In addition to that, non-mobile-app (keypad-based) smart door locks market touched US$88.52 million in 2017 and is projected to maintain its dominance in near future in the Indian subcontinent at US$917.49 million in 2025.

Valued at US$34.09 million in 2017, fingerprint-based smart door lock was the most in demand followed by palm recognition smart door locks. Iris-based smart lock is available in the Indian market but it is expected to show a bleak demand. However it may become popular in metro cities and areas that require heavily guarded security services. Technology using RFID to unlock the door (37.64% share) is still the most popular and would enjoy 33.91% share of the market in 2025.

The commercial sector's demand for smart locks grabbed 61.32% share in 2017 and by 2025 the commercial sector will account for 58.95% share of the total smart door lock market. After the commercial sector, the residential sector is expect to have the second highest share of the market at 41.05% in 2025, up from 38.68% in 2017. SST

Fire Protection Connected To The Cloud

Global technology company Siemens AG has launched Cerberus Portal, a cloud-based online fire protection software to monitor fire systems.

It is the first step the company is taking towards digitalising Siemens fire safety products and is the initial component of the new Cerberus Cloud Apps offering.

Said Johannes Mario Kahlert, Head of Fire Safety at Siemens Smart Infrastructure, "There is an ongoing disruptive revolution in our fire safety industry. That revolution is called digitalisation. I am deeply convinced that digitalisation will change the way we do business."

As a cloud application, Cerberus Portal can be used from any online device – PCs, laptops and tablets running on any operating system. This allows all fire control panel information, such as faults, alarms and general system status, to be accessed remotely.

A simple user interface and a clear overview of all connected sites draw the operator's focus to what is really important: have the fire protection system up and running at all times.

Cerberus Portal is particularly useful in case of an incident. In a system incident, maintenance personnel receives real-time information to react promptly, inform customers and prepare site visits. Real-time data can be examined in detail before service technicians are despatched. Because these technicians know about the issue in advance, they are well prepared and will have the necessary information, tools and equipment when they arrive on site.

The Cerberus Connect X300 gateway makes sure all relevant data is delivered to Cerberus Portal in real time. Leveraging the power of edge computing technology, data is preprocessed locally on the gateway before it is sent to the cloud. Not only can this multi-protocol gateway be connected to both Siemens and third-party building products, it is also easy to install and commission. Encrypted transmission technology and a built-in firewall ensure the highest level of security.

The digitalisation of fire protection systems and related maintenance activities allows service providers to save time and travel expenses. It is estimated that Cerberus Cloud Apps will enable maintenance companies to take care of up to 10% more customers with the same number of staff members.

Kahlert elaborated, "Adding this new technology to our product portfolio will open doors to create new remote services, increase our customer satisfaction rate and imagine new innovative applications such as predictive maintenance." SST

> *"There is an ongoing disruptive revolution in our fire safety industry. That revolution is called digitalisation. I am deeply convinced that digitalisation will change the way we do business."*
>
> ***- Johannes Mario Kahlert, Head of Fire Safety at Siemens Smart Infrastructure***

Security Flaws In Electronic Arts' Origin Platform

►► By Check Point Software Technologies Content Team

With over 300 million users and revenues of around US$5 billion, EA Games is the world's second largest gaming company in terms of market capitalisation. Its portfolio includes household gaming titles such as FIFA, Maden NFL, NBA Live, UFC, The Sims, Battlefield, Command and Conquer and Medal of Honor. All these games and more rest on its self-developed Origin gaming platform, which allows users to purchase and play EA's games on PCs and mobile phones.

Origin also contains social features such as profile management and networking with friends along with community integration with networking sites such as Facebook, Xbox Live, PlayStation Network and Nintendo Network.

Recently Check Point Research combined forces with CyberInt to identify a chain of vulnerabilities that, if exploited, could lead to the takeover of millions of player accounts held by EA Games. Potential damage could have been caused by an attacker gaining access to a user's credit card information or fraudulently making purchases in game currency on behalf of the user.

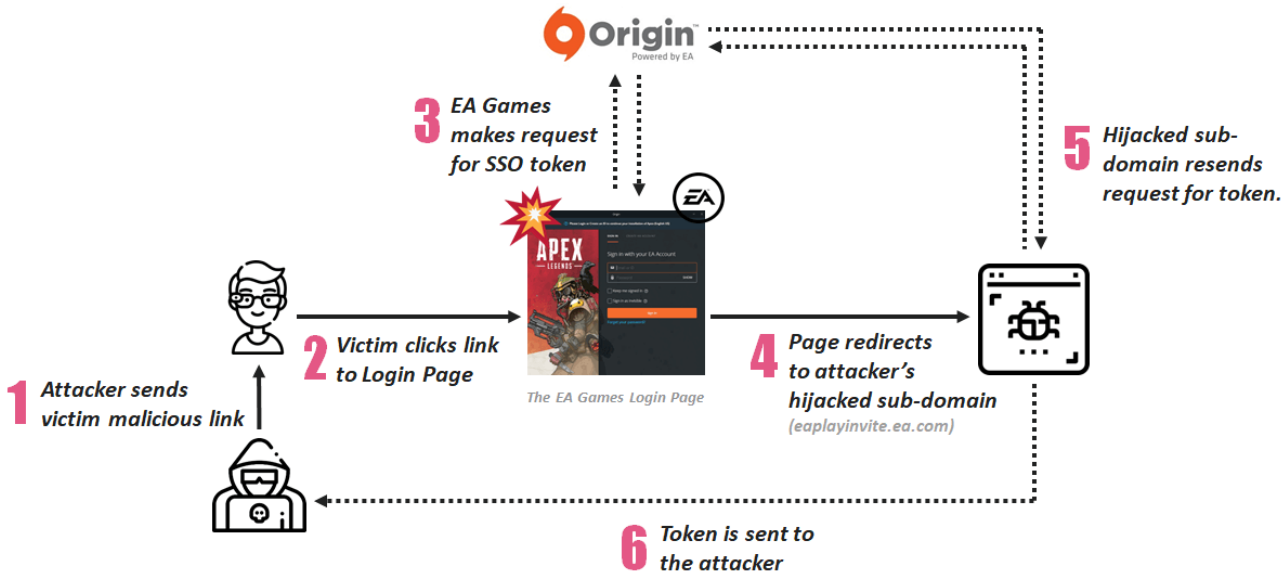
CyberInt and Check Point immediately notified EA Games of these security gaps and together leveraged their expertise to support EA Games in fixing them to protect its gaming customers.

In a similar manner to Check Point Research's previous discoveries into another hugely popular online game, Fortnite, the vulnerabilities found in EA's platform also did not require the user to hand over login details. Instead, the attacker took advantage of EA Games' use of authentication tokens in conjunction with the oAuth Single Sign-On (SSO) and TRUST mechanism that is built into EA Game's user login process.

How The Attack Works

EA Games is a cloud-based company that uses Microsoft Azure to host several domain names such as ea.com and origin.com to provide their players global access to various services including creating new game accounts, connecting to the Origin social network and purchasing more games in EA's online store.

Each service offered by EA is registered on a unique subdomain address, for example, eaplayinvite.ea.com, and has a DNS pointer (A or CNAME record) to a specific cloud supplier host, such as 'ea-invite-reg.azurewebsites.net', which runs the desired service in the background, in this case a web application server.



EA Games is a cloud-based company that uses Microsoft Azure to host several domain names such as ea.com and origin.com to provide their players global access to various services including creating new game accounts, connecting to the Origin social network and purchasing more games in EA's online store.

Due to misconfigurations in the Azure cloud platform however, EA had changed the 'ea-invite-reg-azurewebsites.net' CNAME record so that the subdomain eaplayinvite.com no longer pointed to it. This meant that eaplayinvite.ea.com now leads to a dead link. It was thus very straightforward for our team to purchase the 'ea-invite-reg.azurewebsites.net' CNAME record instead and have eaplayinvite.com point to our own cloud account. As we now controlled this sub-domain, any user accessing this url could now unknowingly be routed through our team's cloud hosting account.

Stage Two Of The Attack

The next step was to understand how EA games had configured the oAuth protocol and provided its users with a Single Sign-on (SSO) mechanism. This SSO mechanism essentially exchanges the user's login credentials (username and password) with a unique SSO Token that is then used to authenticate the user across EA's network without them having to reenter their login details.

After discovering some issues in the way EA had implemented the TRUST mechanism, our team was able to redirect where the SSO Token is sent to and request it to be sent to our EA's hijacked sub-domain, eaplayinvite.ea.com.

The Damage Caused

With the access token now in the hands of the attacker, he can now log in to the user's Origin account and view any data stored there, including the ability to buy more games and accessories at the user's expense. Needless to say, apart from it being a massive invasion of privacy, the financial risks this poses and the potential for fraud is vast.

Key Takeaways

It is important that organisations with customer-facing online portals carry out proper validation checks on the login pages they ask their users to access. They must also perform thorough and regular hygiene checks on their entire IT infrastructure to ensure they have not left outdated or unused domains online. With attackers constantly on the lookout for the weakest link in your company's online presence, these often unknown and unprotected pages can easily serve as a backdoor to your enterprise's main network.

With so much data stored online, especially in the cloud, the way that data is accessed must be thoroughly reviewed and improved on a regular basis. Despite regulations such as GDPR, data breaches via account takeovers still occur on an almost daily basis and the damage they cause can easily affect whether or not an organisation is able to game on. SST

Security Solutions Today

sst.tradelinkmedia.biz

Security Solutions Today (SST) is a leading publication on the latest security information, trends and technology, and products that include Access Control, CCTV/IP Surveillance, Intrusion Detection and Integrated Security Systems.

SST is packed with the latest developments in security technologies and trends, events, previews and reviews of major global trade shows, product launches and security installations worldwide.

What's Hype, What's Reality In Today's Threat Landscape

Speakers at RSA Conference 2019 weigh in on the evolving threat landscape, and uncover what is hype, what is reality and what this means for businesses and CISOs in the Asia Pacific region.

With the continuous emergence of new technologies, enterprises now find themselves having an ever-growing repository of security products that do not necessarily help in providing strategic management of cyber threats. Industry experts participating in RSA Conference 2019, which took place in July in Singapore, shed light on what risks are understated or overstated, so businesses and CISOs can distinguish between hype and what should be genuine priorities.

1. It is possible for a cybersecurity solution to be completely unhackable

The adoption of fraud detection and prevention solutions, including multi-factor authentication and biometric solutions, is on the rise in Asia. While such solutions buffer against attacks, experts caution that businesses need to do more than just ensure that technologies are in place. "The reality is, biometrics also brings with it some caveats and new risks, including privacy concerns around how 'Personal Identifiable Information' is collected, shared and secured as this data can also be a target for cybercriminals. As biometric technologies depend on probabilities and confidence scores, there are also risks that the systems can be spoofed by say, a photo. Therefore, it is always best for biometrics to work in conjunction with other security measures," explained Vicky Ray, Principal Researcher, Unit 42 Threat Intelligence, Asia Pacific.

An executive advisor of a Fortune 100 company and member of the RSAC Program Committee shared similar sentiments. "We have seen security 'silver bullets' come and go over the years. It used to be biometrics and now vendors are praising AI as the ultimate cyber defence weapon. Unfortunately, the one constant is that hackers will resolve to targeting the weakest link - people. While biometrics are good as another layer of security, it is just an additional layer of security. If hackers can convince people to do something that they should not do, no technology will help," he stated.

2. When IoT devices are embedded with security vulnerabilities, it puts users at risk

The opportunities that the Internet of Things phenomenon

> *"The challenges that security professionals have been facing with legacy systems is their complexity and lack of security by design, which necessitate off-network operations. This is still a common practice as it reduces critical systems exposure, providing mitigating controls by limiting potential cyber attacks through segregation."*
>
> ***- Magda Lilia Chelly, Managing Director at Responsible Cyber Pte Ltd***

offer businesses and industries is almost unparalleled, with ubiquitous connected devices providing key physical data that unlock further business insights via the cloud. Yet, they have also become a security concern because of the emergence of distributed denial of service attacks and a rising number of internet security breaches launched against servers.

Experts warn that this is a valid concern, and that more needs to be done in order to protect end users. Sunil Varkey, Chief Technology Officer and Security Strategist, Middle East, Africa and Eastern Europe, Symantec, said, "Even as IoT adoption is in a rapid phase and may soon touch our everyday lives, security needs to be accounted for. Currently, it is not a major consideration in the development lifecycle. As such, most security practitioners are not yet familiar with security protocols for IoT, and that needs to change. Otherwise any exploit on the vulnerabilities or misconfigurations could have a huge impact on safety."

Srinivas Bhattiprolu, Senior Director-Solutions and Services, Asia Pacific-Japan, Nokia, elaborated on how threat actors could potentially target IoT devices, as indicated by the fact that lateral movements to compromise assets within the security perimeter have been on the rise. "In order to secure an end-to-end IoT system, it is necessary to clearly understand the vulnerabilities and exploits associated with specific components as well as of the system as a whole," he stressed.

3. Critical infrastructure owners should create separate networks to move essential operations off the internet

In recent years, governments and organisations across the APJ region have begun the introduction of separate networks, and have even cut off internet connection from employees' devices in order to prevent potential leaks from e-mails and shared documents. The Singapore government's move in May 2017 is one such measure to prevent attackers from tapping the internet to plant malware in work devices. As to whether this is essential, experts hold differing views.

"The challenges that security professionals have been facing with legacy systems is their complexity and lack of security by design, which necessitate off-network operations. This is still a common practice as it reduces critical systems exposure, providing mitigating controls by limiting potential cyber attacks through segregation," explained Magda Lilia Chelly, Managing Director at Responsible Cyber Pte Ltd.

Sunil Varkey however pointed out the increasing challenge of this practice. "While isolation and separation of network segments was an active defence strategy when systems and information were well within defined perimeters and enterprise networks, this might not be enough to solve challenges anymore. This is because heterogeneous multi-cloud environments see users having multiple IT personas."

"Beyond segregation, owners and operators of critical infrastructure should make sure their systems are properly secured, patched, updated and monitored. It is too easy for an individual today to go on one of several search engines and easily find misconfigured or unpatched critical systems," continued Varkey.

4. AI-powered systems are self-sustaining and secure by design

According to market research firm Reportlinker, the Asia Pacific region is expected to be the largest AI cybersecurity market as a result of the high adoption of advanced technologies like IoT, big data and cloud computing. As for its ability to keep out attacks, experts warn that AI has both sped up advances in cybersecurity solutions and exacerbated the threat of cybercrime.

"We have seen recent AI deployments across cybersecurity solutions, where companies claim that they can detect attacks faster using the technology. Academic research proves a success rate between 85% and 99% depending on the implementation, algorithms and data," highlighted Magda Lilia Chelly.

"In order for AI to be successful, it requires the appropriate data input. If the data input is manipulated or biased, new security concerns can emerge very quickly," she added. SST

Teaching Cars To Fly

By 2030, people around the world will take one billion flights in air taxis. What is more, most of those air taxis will be operating without a pilot. Bosch, a global supplier of technology and services, is helping make this future a reality.

With traffic jams a common occurrence in the world's cities, frustrated drivers sometimes find themselves looking to the heavens for a little help from above. A few years from now, the skies could indeed be a solution.

"Compared to today's means of transportation, flying taxis save time on trips of 10 kilometers or more, with a maximum range of up to 300 kilometers," according to Marcus Parentis, head of the technology team at Bosch in charge of the control units behind the electric light aircraft.

The Boston Consulting Group predicts that people around the world will take one billion flights in air taxis in 2030 once air taxi sharing services have been established along fixed routes above the ground. What is more, most of those air taxis will be capable of operating without a pilot.

All Up In The Air: One Billion Flights In Flying Taxis

The market for flights using electric air taxis in cities is set to see substantial growth in the years ahead. Test flights are scheduled to begin in cities such as Dubai, Los Angeles, Dallas and Singapore in 2020. Experts expect commercial operations to begin in 2023. Light aircraft could start flying autonomously over the roofs of major cities as early as 2025, controlled by staff on the ground.

By that time, roughly 3,000 flying taxis will be in operation worldwide, according to global strategy consulting firm Roland Berger. That number will increase to 12,000 by 2030, with just under 100,000 flying taxis taking to the skies by 2050.

Consultants from Morgan Stanley estimate that the market for flying taxis could even reach €1.35 trillion (US$1.5 trillion) by 2040, extending beyond the United States and Southeast Asia to include large and medium-sized cities in Germany as well.

In regions such as the Ruhr valley, the Frankfurt Rhine-Main metropolitan region, and the Munich/Augsburg/Ingolstadt metroplex, they have the potential to significantly speed up travel over short and medium distances.

Marcus Parentis of Bosch believes in the growing market opportunities. "We are talking to air taxi manufacturers from the aerospace and automotive industries, as well as with startups that build air vehicles and are looking to provide sharing services. The question isn't whether flying taxis will become reality but when."

"Bosch plans to play a leading role in shaping this future market," said Harald Kröger, president of the Bosch Automotive Electronics division.

Specifically Bosch is working on state-of-the-art sensor technology to make these flights safe, comfortable, and convenient.

Why the focus on sensors? Bosch thinks it has discovered a gap in the market. Conventional aerospace technology is too expensive, bulky and heavy to be used in autonomous flying taxis. However, modern sensors that are also used for automated driving or in the ESP anti-skid system may potentially be able to bridge this gap.

Bosch Technology For Flying Taxis

At Bosch, a team of engineers has combined dozens of sensors to create a universal control unit for flying taxis. Featuring Bosch sensors already in use in production vehicles, the universal control unit is designed to ensure the ability to determine the position of the flying taxis at all times, allowing them to be controlled with precision and safety.

Acceleration and yaw-rate sensors that accurately measure the flying vehicles' movements and angle of attack, for example, provide necessary data. Unlike current sensor systems in the aerospace sector, some of which cost tens of thousands or even several hundred thousand euros, Bosch offers sensor solutions at a fraction of the cost. That is because Bosch uses production-tested sensors that the company has already been developing and manufacturing for the automotive industry for many years.

The Bosch sensors are especially small and lightweight. Flying taxi manufacturers can easily install the Bosch sensor box into their air vehicles using the plug-and-play principle. Bosch's plug-and-play control unit fits in any flying vehicle.

Bosch is in contact with a wide range of players in this field, from air taxi manufacturers to startups looking to build air vehicles and provide sharing services.

The Bosch sensor box is equipped with MEMS sensors. The abbreviation MEMS stands for microelectromechanical systems. Bosch developed the first MEMS sensors for vehicles over 25 years ago. In vehicles, they supply control units with data about whether the car is currently braking or accelerating, and lets them know the direction in which the vehicle is travelling. The Bosch sensor box for flying taxis is equipped with acceleration sensors that measure the movements of the aircraft. Built-in yaw-rate sensors measure the flying vehicle's angle of attack, while magnetic field sensors gauge its compass heading.

The package also includes pressure sensors, which use barometric pressure to measure altitude and dynamic pressure readings to determine the vehicle's current speed.

How Much Will Flying Taxis Cost?

It is important for suppliers to provide reliable technology that is not only lightweight and easy to install, but also offers an economic advantage compared to traditional aerospace technology. "That's where our MEMS sensor box comes in. Through our Bosch solution, we aim to make civil aviation with flying taxis affordable for a wide range of providers," Parentis said.

Depending on the concept and number of passengers carried, a flying taxi will cost around €500,000. This is far less than the cost of a comparable helicopter equipped with today's technology.

As with any new technology, there is currently different concepts on offer. At the present time, it is hard to say which concept will come out on top. SST

- Forecast is one billion flights in flying taxis in 2030.
- Bosch sensor box makes it possible to control flying taxis with precision.
- Sensor solution from Bosch is cheap because it uses production-tested components meant for the automotive sector.

Sensor box for air taxis

FLYING HIGH
Starting from 2023 at the latest, the first autonomous air taxis will take off in major cities. For those electrically powered air taxis Bosch is developing a universal control unit with modern sensor technology. These sensors make flights particularly safe and comfortable. Automotive sensors deliver highly reliability at low cost.

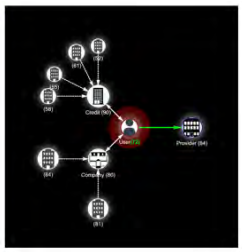
about
1.000.000.000
Passenger flights in air taxis in 2030*

*source: BCG 2018

BOSCH
Invented for life

New Fujitsu Technology Enables Safer Online Transactions By Confirming Trustworthiness Of Personal Credentials

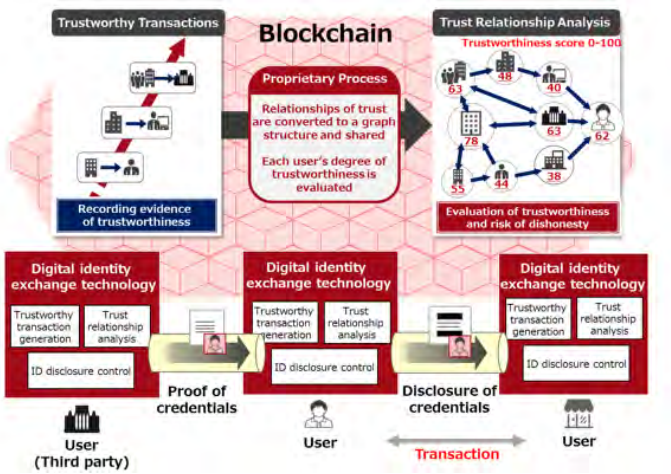
Fujitsu Laboratories Ltd. has developed a digital identity exchange technology that evaluates trustworthiness in online transactions. The technology makes it possible for individual users and service businesses involved in online transactions to confirm the identity of other parties in transactions.



The technology promises a future in which people can enjoy online services more safely.

In recent years, there has been an increase in new forms of business based on trust between people or companies, including sharing and matching services. In these sorts of digital businesses, it is vital to accurately convey the identity of the other party in the transaction. When users cannot see the other party face to face, it is difficult to judge the credibility of the other party, causing concerns about trust.

With reports of fraud and instances of people falsifying personal credentials like work history and professional qualifications increasingly prevalent, ensuring the circulation of high-quality, reliable identification data is an urgent challenge for users and businesses alike.



To address this, Fujitsu Laboratories has developed a technology based on Decentralised Identification (DID). DID is a scheme where a user can disclose his personal credentials to other parties with certification provided by an impartial third party. Fujitsu Laboratories' new technology utilises blockchain that analyses the risk of falsification and the trustworthiness of the other party's personal credentials when a user conducts a transaction online. The technology achieves this through a mutual evaluation of the users when a transaction occurs, and by inferring the relationships between users based on past transaction data.

Users can have their credentials verified with only a partial disclosure of relevant data, allowing for safe and highly reliable transactions without forcing users to offer unnecessary personal details.

This technology include user-friendly features such as graphics to visualise the relationships between users, as well as a unique 'trust score' that make it easier to determine each user's trustworthiness before starting a transaction. A trustworthiness score is attached to each user by weighing factors including how many trusted users evaluate them highly. Even if a user colludes with a third party to improperly raise the user's evaluation, the relationship graph will reveal information such as the weakness of the user's relationships with other users, giving the system the potential to identify misrepresentations.

Fujitsu Laboratories will continue to develop IDYX as a trust-based service platform supporting digital business. It will conduct trials in various sectors, starting with the finance industry. In addition, Fujitsu aims to implement this technology in 2019 as a new functionality in its Fujitsu Intelligent Data Service Virtuora DX Data Distribution and Utilization Service, a cloud-based solution for data utilisation powered by blockchain technology. SST

Fire Safety Event 2019
9 - 11 April 2019
The NEC,
Birmingham, United Kingdom

The Fire Safety Event 2019 Hailed A Huge Success

The Fire Safety Event 2019 was the most successful edition to date. The event drew 11,733 visitors across three days at the NEC, Birmingham, England, firmly cementing its stature as the fastest growing exhibition in the UK for the industry.

High-profile incidents in recent years have put a spotlight on the industry and The Fire Safety Event recognises it has a role to provide ongoing education on new standards and legislation, best practice advice and giving industry access to companies and products that will better prepare them.

The Fire Safety Event has grown vigorously since its inception in 2017. The event, which began with 16 exhibitors, boasted over 50 this year. The exhibitor line-up for 2019 included Advanced, asecos, c-Tec, Checkmate Fire Solutions Ltd, FFE Limited, Fike Safety Technology Ltd, FireClass, FirePro UK Ltd, Kingspan, Klaxon, Turner & Townsend, WAGNER UK Ltd and Xtralis UK Ltd.

The event received high praise from both exhibitors and visitors. Ian Rose, Director of Global Fire Equipment (UK) commented, “The Fire Safety Event is fast becoming the key fire industry exhibition to attend for both visitors and exhibitors alike.”

The exhibition featured seminars and exhibitors. With 67% of visitors also pre-registering for seminars, The Fire Safety Event is fulfilling the desire within the industry for the latest product innovations, best practice and advice on legislative changes.

Particularly noteworthy this year were the numerous specialist demonstrations on offer - such as the live burn tests from Kingspan and asecos’ DSEAR with a Bang Demo Area.

Brand new for 2019 and a great success was the Tall Building Fire Protection Area hosted by the Association for Specialist Fire Protection. This feature brought together expert speakers from across the industry. Throughout the full three-day duration, this Protection Area was a hive of activity. SST

Subscription Form

Fax your order today
+65 6842 2581

(Please tick in the boxes)

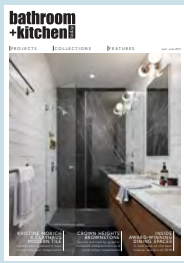
Southeast Asia Building

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: _____

ADVERTISER INDEX

PLATINUM PARTNER

Dahua Technology	Singapore	+65 6538 0952	sales.sg@dahuatech.com	www.dahuasecurity.com	IFC

GOLD PARTNERS

Microengine Technology	Malaysia	+603 7957 2008	enquiry@microengine.net	www.microengine.net	5
Delta Scientific	U.S.A.	+1 661 575 1100	info@DeltaScientific.com	deltascientific.com	3

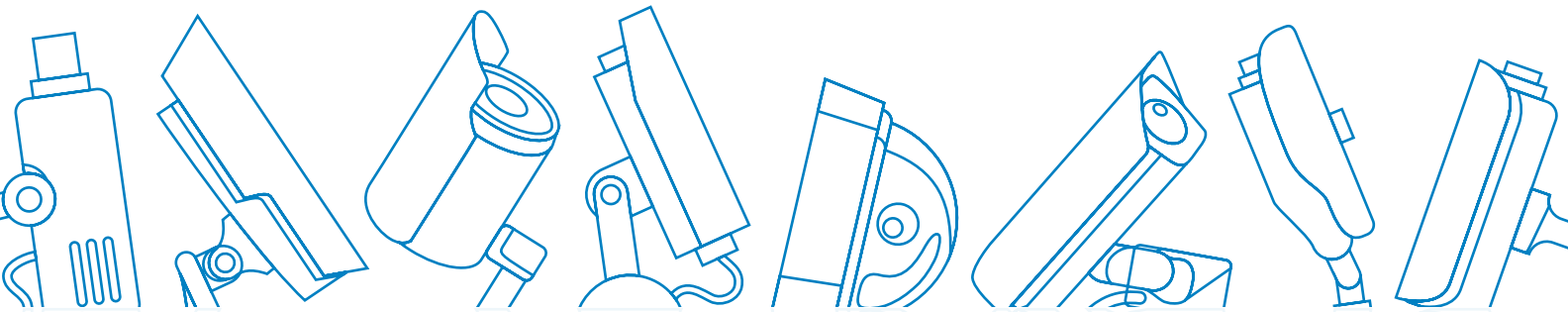
SILVER PARTNER

Axxonsoft Asia Pte Ltd	Singapore	+65 6536 9102	info@axxonsoft.com	www.axxonsoft.com	OBC

See us at following upcoming events!

Event	Date	City	Country	Website	Page
Secutech Vietnam 2019	14 – 16 Aug 2019	Ho Chi Minh City	Vietnam	www.secutechvietnam.com	11
Smart Cities & Buildings Asia 2019 / IBEW 2019	4 – 6 Sept 2019	Singapore	Singapore	www.scb-asia.com	7
GSX 2019	8 –12 Sept 2019	Chicago, IL	U.S.A	www.gsx.org	19
Safety & Security Asia 2019	1 – 3 Oct 2019	Singapore	Singapore	www.safetysecurityasia.com.sg	1
Secutech Thailand 2019	28 – 31 Oct 2019	Bangkok	Thailand	www.secutechthailand.com	9
IFSEC International 2020	19 – 21 May 2020	London	United Kingdom	www.ifsec.events/international/	13
IFSEC SEA 2020	23 – 25 Jun 2020	Kuala Lumpur	Malaysia	www.ifsec.events/kl/	15
IFSEC Philippines 2020	22 – 24 July 2020	Manila	Philippines	www.ifsec.events/philippines/	17

Our tribute to Safety & Security...



TradeCards Global mobile application is offering **50% discount** for one-year organisation listing to suppliers and service providers that serve our Safety & Security Community. With the reduced price of USD500 / *SGD700 for one-year organisation listing, suppliers and service providers get to enjoy an ***additional 10MB of product listing*** tagged to your organisation listing.

Visit **www.tradecardsglobal.com** to sign up for a new account and your organisation listing. Input "**SECURETRIBUTE**" as promo code before proceeding to payment page. The promo code is valid until 31 December 2019.

*Rate excludes 7% GST applicable for Singapore-registered companies

TRADECARDS GLOBAL

Supporting mobile version of:

SEAB SOUTHEAST ASIA BUILDING · SOUTHEAST ASIA CONSTRUCTION · Security Solutions Today · bathroom +kitchen today · lighting today

GET IT ON Google Play

Download on the App Store

AUTO — RETAIL — FACE

Intellect

ACFA — RAILWAY — ATM

Physical
Security
Information
Management

Intellect PSIM

REACTION
OBJECTS
STATUS
EVENT

SYSTEM CORE
CONTROL LOGIC

USERS
DB
INCIDENTS & EVIDENCE HANDLING
SITUATIONAL AWARENESS

THE OPEN PLATFORM SOFTWARE

SDK

VIDEO ANALYTICS
3rd PARTY APPLICATIONS

FIRE ALARM
BMS/BAS
PIDS/FIDS
PLC/SCADA
INTRUSION ALARM
ACCESS CONTROL SYSTEM
INTERCOM
I/O DEVICES
PUBLIC ADDRESS

MACRO
SCENARIO CHECK & RESPONSE
SCRIPT

DATA PRESENTATION (VISUAL & AURAL)
INTERACTIVE MAPS
REPORT MANAGEMENT
AUDIT TRAIL

FACE

FACIAL RECOGNITION AND FACE SEARCH

AUTO

LICENSE PLATE RECOGNITION AND TRAFFIC MONITORING

UNLIMITED SCALABLE DISTRIBUTED ARCHITECTURE

FOUR LEVELS OF AUTOMATION

LOW-LEVEL INTEGRATION WITH EDGE DEVICES

Access control	IP devices	Fire and security alarm	Perimeter security
40+ systems	**10,000+** models	**40+** systems	**15+** systems

axxonsoft
EXPERIENCE THE NEXT®

Axxonsoft Asia Pte Ltd
Learn more
www.axxonsoft.com