Security Solutions Today

May / June 2019

REAL SMART BUILDINGS, REAL SMART CHANGES

WITH SMART BUILDINGS, NEW POSSIBILITIES EMERGE EVERY DAY

Cover Story

Smart buildings usher in a connected future

Inside Look

Have biometric applications reached a security tipping point?

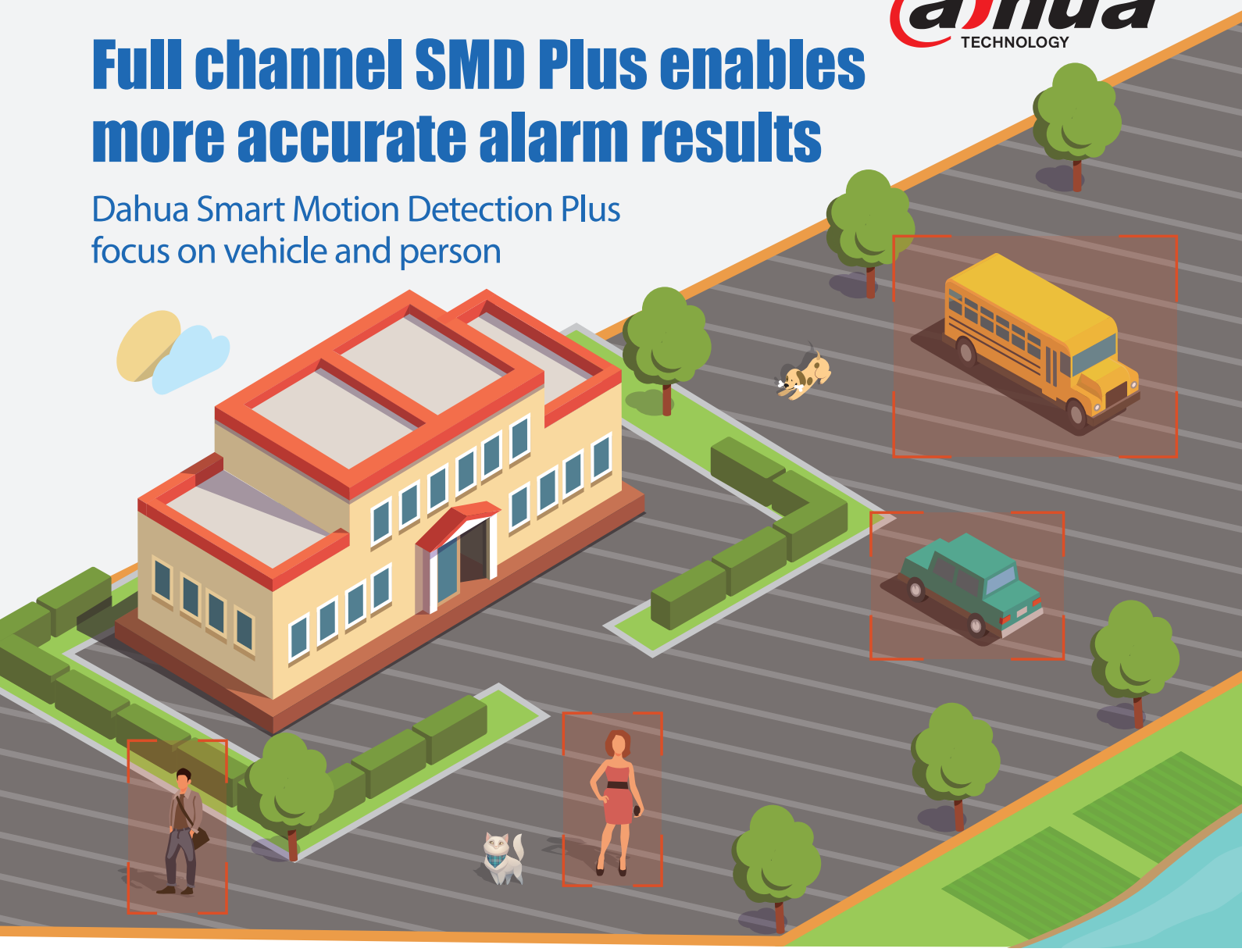
Inside Focus

Study: 96% of Singaporean businesses breached

Scan this to download the latest issue from our website

Full channel SMD Plus enables more accurate alarm results

Dahua Smart Motion Detection Plus focus on vehicle and person



- Embedded AI chip with the deep learning algorithm providing 10 times computing power to upgrade full channel SMD Plus function with up to 95% accuracy
- Send alarm only when person and vehicle intrude and filter out false alarms caused by light & leaves, applicable to indoor & outdoor scenarios
- Person & Vehicle optional for playback to achieve quick target search, saving event retrieval time
- Actively warns off intruders with SMD Plus triggered flashlight and siren

Recommended Models

XVR7000-4KL-I Series
HDCVI 4K & H.265 AI XVR

XVR5000-I Series
HDCVI 1080P & H.265 AI XVR

HAC-ME1500/2241C
HDCVI Active Deterrence Camera

HAC-ME1500/1200D
HDCVI Active Deterrence Camera

CE FC RoHS UL ISO 9001:2000

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

INTERPOL WORLD 2019

www.interpol-world.com

ENGAGING CO-CREATION TO PREPARE FOR FUTURE SECURITY THREATS

2 - 4 July 2019

Sands Expo & Convention Centre • Singapore

Key Highlights at INTERPOL World 2019

More than **30** Co-creation Labs

More than **200** International Exhibitors

8,000 Attendees

4 National Pavilions

4 Working Groups *(by invite only)*

Meet the Keynote Speakers:

Richard van Hooijdonk
International keynote speaker, crime and technology trendwatcher and futurist
The Netherlands

Dr Mary Aiken
Cyberpsychologist and academic advisor
Europol's European Cyber Crime Centre (EC3)
United Kingdom

Learn and Contribute to These Topics and More at the Co-creation Labs:

2 July 2019
- Regulating Big Data
- Partnerships
- Data Fusion

3 July 2019
- Future Capabilities and Cultures
- Border Security
- Community Participation

4 July 2019
- Smart Cities
- Cyber Disruptors & Drivers of Change
- Privacy

Register by 31 May to enjoy Early Bird Rates!

visitor@interpol-world.com

#INTERPOLWorld

EVENT OWNER: INTERPOL

SUPPORTED BY: Ministry of Home Affairs Singapore; Singapore Exhibition & Convention Bureau

INDUSTRY INSIGHTS BY: pwc

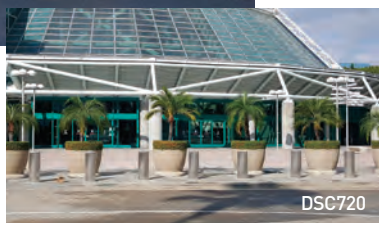
HELD IN: Singapore – Passion Made Possible

MANAGED BY: imp

IN THIS ISSUE

You asked for it; **DELTA** made it.

MP5000



DSC720

The lighter weight DC-operated, M30 certified Delta DSC1500 portable beam barricade is now available. With a clear opening of 16 feet (4.8 m), the DSC1500 easily and temporarily secures locations where roads need closing down to one or two lanes, deters thefts from parking lots and protects anywhere a beam barricade is needed for short-term security.

Learn more about the DSC1500 and discover all of the security solutions offered by Delta at **www.deltascientific.com**.

For holding events, keep pedestrians and staff safe with Delta's full line of portable barricades and bollards. See them at www.deltascientific.com.

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)

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
ISSN 2345-7104 (Print)

Printed in Singapore by Refine Printing Pte Ltd

ANNUAL SUBSCRIPTION:

Surface Mail:

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

Airmail:

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

ADVERTISING SALES OFFICES

Head Office:
Trade Link Media Pte Ltd *(Co. Reg. No: 199204277K)*
101 Lorong 23, Geylang, #06-04, Prosper House,
Singapore 388399
Tel: +65 6842 2580 Fax: +65 6842 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

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...

MAY

Secutech 2019

Date: 8 - 10 May 2019
Venue: Taipei Nangang Exhibition Center, Taipei, Taiwan
Telephone: +886 2 8729 1099
Website: www.secutech.com
Email: services@secutech.com

JUNE

IFSEC Philippines 2019

Date: 13 - 15 June 2019
Venue: SMX Convention Centre, Pasay City, Metro Manila, Philippines
Telephone: +63 2 551-7718 / 839-1306
Website: www.ifsecphilippines.com
Email: info-ph@ubm.com

JUNE

IFSEC International 2019

Date: 18 - 20 June 2019
Venue: ExCeL London, London, UK
Telephone: +44 (0) 20 7921 5000
Website: www.ifsec.events/international/
Email: ifseccustomerservice@ubm.com

JULY

INTERPOL World 2019

Date: 2 - 4 July 2019
Venue: Sands Expo and Convention Centre, Singapore
Telephone: +65 6389 6613
Website: www.interpol-world.com
Email: layeng.see@interpol-world.com

JUNE

BMAM Expo Asia 2019

Date: 27 - 29 June 2019
Venue: IMPACT Exhibition Center, Hall 6, Bangkok, Thailand
Telephone: +66 8 6561 3344 / +66 2833 5111
Website: www.bmamexpoasia.com
Email: radcharinn@impact.co.th

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

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

SEPTEMBER

Bex Asia 2019

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

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

avigilon™
a Motorola Solutions Company

AI Delivering Actionable Results

Complete Video Surveillance and Access Control Solutions

Transportation is a complex ecosystem that is part of the critical infrastructure of any city — and a disruption to transport networks can have an immediate and significant impact on citizens and the economy. Avigilon provides complete security solutions that are powered by artificial intelligence to address the security challenges of the transportation industry and help reduce the number of transportation-related interruptions in day-to-day operations.

Superior Preventative Protection

Avigilon self-learning video analytics allow a single operator to focus their attention on the events that matter most, along with alarms and rule triggers that provide immediate notifications to suspicious activities for responses in near real-time.

Cost-Effective Security

Avigilon ultra-high definition surveillance cameras allow coverage of wider areas with fewer cameras, and Avigilon High Definition Stream Management (HDSM)™ and HDSM SmartCodec™ technologies maintain exceptional image quality while reducing network bandwidth and storage capacity needs.

Powerful Search

Avigilon Control Center™ video management software with Avigilon Appearance Search™ technology sorts through hours of video with ease to quickly locate a specific person or vehicle of interest.

avigilon.com/transportation | asksales@avigilon.com

EDITOR'S NOTE

Dear esteemed reader,

Smart buildings are shaping our future in exciting ways. Not just a roof over our head, they are also the basic building blocks of smart cities. The transforming of cities into smart cities begins when they become populated with smart buildings.

But what makes a building smart? A smart building is one that uses technologies to automate building management and to deliver useful, integrated and smart services that make occupants productive at the lowest cost and with the least environmental impact over the building's life cycle.

For instance, using data provided by sensors, which is then crunched, smart buildings know when and where to carry out repair works and will alert facility managers accordingly. Furthermore, with smart buildings, manual control of a building's heating and cooling is no longer required.

In short, smart building technology and automation are now able to give the humans living and working inside them the perfect environment to thrive, be happy and be productive.

With smart buildings, the once unimaginable is now upon us, and the possibilities are truly boundless.

Michelle Lee

Editor

IFSEC PHILIPPINES

SECURITY • FIRE • SAFETY

13 - 15 JUNE 2019

SMX CONVENTION CENTRE
PASAY CITY, METRO MANILA

Organised By

UBM

THE LEADING
SECURITY, FIRE & SAFETY
EVENT IN THE PHILIPPINES

EMPOWERING THE PHILIPPINES TO BE THE SAFER NATION BY PROVIDING GLOBAL INNOVATION AND EXPERTISE TO THE EMERGING TRENDS AND SERVICES IN SECURITY, FIRE AND SAFETY MARKETS.

WWW.IFSECPHILIPPINES.COM

@IFSECPHILIPPINES #IFSECPHILIPPINES IFSECPHILIPPINES

Axis' All-In-One Door Station Combines Video Surveillance, Door Communication And Integrated RFID Reader

Axis Communications has launched a new door station that serves as a multifunctional device, covering every need at the door.

The AXIS A8207-VE Network Video Door Station combines video surveillance, door communication and an integrated RFID reader for access control in a single, easy-to-manage device.

The product brings added value to security solutions by functioning as a bridge between video surveillance and access control. The door station combines a fully featured 6 MP network camera with two-way audio communication and remote entry control. It also has an integrated RFID reader and supports video and audio analytics, such as motion or sound-based detection for triggering events or recordings.

Based on open standards and with several hardware interfaces, the door station easily integrates with other systems and solutions. In addition, an induction loop for hearing aids makes interaction accessible for people with hearing loss.

One example of how it works: At a university faculty building, students and other visitors can use the door station to call the professor they are visiting to gain access. Meanwhile security personnel can use the video from the door station as part of their surveillance setup and to interact with people during emergency situations or to provide general guidance.

AXIS A8207-VE is also useful for back doors and loading docks in retail settings.

The integrated reader allows employees to enter their workplace without anyone having to run to the back of the store to let them in, eliminating the need for widespread key distribution, which could lead to keys easily getting lost or stolen and ending up in unauthorised hands. Known suppliers can have their own access card or PIN to only enter the building during office hours, while unknown suppliers can use the call button to ring store personnel, who can answer through a normal desk phone or mobile app and grant access.

After hours, store personnel might have to leave through the back door, sometimes with cash to deposit at the bank. The HDMI output on the door station makes it easy to hook up a live display for staff to check that it is safe to exit before they open the back door. This reduces the risk of an assault while enhancing staffs' sense of personal safety. SST

27-29 JUNE 19

IMPACT Exhibition Center, Hall 6, Bangkok, Thailand

BMAM EXPO ASIA 2019

THE BUILDING & FM EXPO

5,000 Sq.m.
Exhibition space

150
Exhibitors

4,000+
Qualified visitors

Book Your Stand
Now!

Contact: Ms. Radcharin Nuttayakul (Tucky)
M: +66 (0)8 6561-3344 T:+66 (0)2 833-5111 E: radcharinn@impact.co.th

Follow us on
BMAM Expo Asia

Organizer
IMPACT MUANG THONG THANI

Video Control Centre Powered By Focus

Avigilon has launched its new video management software with a promise that it will enhance user interaction and situational awareness through a feature called Focus of Attention.

Combined with other features such as AI-powered analytics and dark mode, the Avigilon Control Center (ACC) 7 ensures that critical events do not go unnoticed.

Focus Of Attention

A new concept in live video monitoring, Focus of Attention leverages AI and video analytics technologies to determine what information is important and should be presented to security operators.

AI-Powered Analytics

Self-learning video analytics and Unusual Motion Detection technologies allow ACC 7 to focus the operator's attention on the most important events.

Dark Mode

ACC 7 delivers colours specifically chosen to reduce eye strain in dark environments like video surveillance control rooms. SST

secutech

8 – 10 May 2019, Taipei, Taiwan
www.secutech.com

Bringing Asia's security, IoT & AI ecosystem together under a single roof

7 Smart solution pavilions

- Smart Retail
- Smart Hotel
- Smart Factory
- Smart Parking
- Smart Healthcare
- Smart Community
- Smart Transportation

7 Thematic zones

1. AI+Software Zone
2. RFID Applications Zone
3. LPWAN Applications Pavilion
4. Smart Lock Pavilion
5. Cybersecurity Pavilion
6. Police Equipment Zone
7. Smart Factory & Industrial Safety

MOBILITY powered by Secutech

- Asia's leading fair for Intelligent Transport Systems
- Showcasing solutions that range from smart road, smart railway, smart parking to fleet management

SMART BIoT SOLUTION powered by Secutech

- Asia's first event for the 'Smart Building Internet of Things'
- Focusing on four major applications: residential & community, hospitality, nursing facility and commercial building

fire & safety powered by Secutech

- Highlighting a full range of solutions from natural disaster monitoring, safe city, industrial safety to personal safety
- Advanced smart disaster prevention applications

info security powered by Secutech

- Revealing the latest cybersecurity solution for the IoT

messe frankfurt

Android-Based Mobile Fingerprint Enrolment Solutions From Suprema ID

Global provider of biometrics and ID solutions Suprema ID has extended its suite of products to include scanners that are compatible with Android systems.

Suprema ID RealScan-D

Suprema ID RealScan-G10

The company's RealScan-G10 and RealScan-D series scanners are compatible with Android to realise greater mobility. For instance, enrolment kits can now be dramatically downsized because laptops can be replaced with compact mobile devices such as tablets and smartphones.

The shift to Android also solves the constraints of limited power supply in outdoor scenarios. In addition, the Android solution supports core technologies such as Machine Learning Live Fingerprint Detection and Multi Dynamic Range without any compromise in enrolment performance.

RealScan-G10 and RealScan-D scanners made their debut at ConnectID 2019 show in Washington, DC on April 30 and May 1.

Suprema ID is involved in national ID projects in 20 countries, with more than one billion people using Suprema ID fingerprinting technology. SST

Modular Surge Protector Takes Away The Guesswork

The Deflector Series Surge Protective Devices from DITEK takes the guesswork out of surge protection by notifying the user three ways when it's time for servicing, setting a new standard for surge protection.

DTK-DF120S1

When the Deflector does its job by absorbing a power surge and stops functioning, the unit sounds a loud audible alarm and an LED flashes, indicating that the module needs to be replaced. Intelligent notification is also available via dry contacts, which can be connected to alarm panels to alert central station monitoring that the module needs replacing.

Said Jason Klein, National Sales Manager at the provider of surge protection solutions, "With the Deflector Series, you'll always know when the surge protection on your critical devices and systems requires immediate attention."

Unique rapid-replacement modules make it possible to have the unit up and running again in only a few seconds.

The DTK-DF120S1 Deflector Series Surge Protector is a 120-volt dedicated circuit protection device designed to minimise damage from AC supply voltage spikes by isolating incoming surges that originate from lightning strikes and other sources. The Deflector is conveniently wall-mountable and simple for a licensed electrician to install. No additional enclosure is required, allowing it to be placed in close proximity to core systems or devices that warrant the highest levels of protection.

The Deflector Series is UL1449 listed as a Surge Protective Device (SPD), as well as UL1283 listed for EMI/RFI noise filtering. SST

4 – 6 SEPTEMBER 2019
SANDS EXPO & CONVENTION CENTRE
SINGAPORE

YOU'RE INVITED!

TO THE REGION'S LEADING EXHIBITIONS FOR THE ENTIRE BUILT ENVIRONMENT VALUE CHAIN

SUSTAINABILITY	ENERGY EFFICIENCY	PRODUCTIVITY	SMART
BEX ASIA	mce ASIA mostra convegno expocomfort	INNO BUILD ASIA	SMART CITIES & BUILDINGS ASIA

WHAT'S NEW THIS YEAR!

First fully integrated exhibitions in the region covering the entire built environment value chain

2 newly launched exhibitions focusing on productivity and smart

Cutting edge sustainability, energy efficiency, construction and smart **technologies that are new in the market**

Specially curated feature to showcase the future of smart buildings

REGISTER NOW TO MEET YOUR FELLOW BUILT ENVIRONMENT PROFESSIONALS

T : +65 6780 4594
E : info@bex-asia.com
W : www.builtenvironmentexpo.com

Exhibitions Organiser

Reed Exhibitions®

IBEW Organiser

Building and Construction Authority

4 Anchor Exhibitions Under

IBEW

CHeKT Bridge Named Best Commercial Monitoring Product At ISC West

The CHeKT Bridge is named the 2019 Commercial Monitoring Product of the Year at the 2019 SIA New Product Showcase Awards, the award show at ISC West that recognises innovative security products, services and solutions.

ISC West is the largest converged security trade show in the US. In 2019 the 30 judges for the award show reviewed more than 95 entries from more than 80 companies for technologies covering more than 30 product and service categories.

The CHeKT Bridge is a revolutionary hardware device that allows a professional security integrator to 'bridge' any alarm panel to any ONVIF compliant camera or recorder. Developed by CHeKT, provider of a visual-monitoring platform for alarm monitoring centres, the CHeKT Bridge pairs on-site cameras with sensors on new or existing security panels.

The platform-agnostic Bridge manages cameras locally allowing an operator to access video instantly, unencumbered by firewalls and login credentials.

When a sensor of any kind goes into an alarm state, the Alarm Inputs on the Bridge record pre- and post-alarm video of the event and immediately upload this to the CHeKT Monitoring portal. Simultaneously, the bridge sends the applicable video to the cloud for viewing by the operator processing the alarm, enabling visual verification of the situation and premises within five seconds.

This powerful simplistic approach allows central stations to provide a much higher level of service without increasing signal traffic or increasing the time an operator spends processing an alarm signal. The operator can forward the clip, via SMS text, to the emergency contacts when additional verification is necessary, and to the police responding to the alarm. SST

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

New Products Boost NetWay Series' Power And Flexibility

Altronix, a provider of power and data transmission solutions for the professional security industry, has added several powerful and flexible new solutions to its NetWay range of solutions.

The new products include three new 8-port Midspans with more power, a Gigabit (1Gb) Ethernet repeater for extended cable runs and a versatile 5-port Ethernet switch that significantly reduces installation and equipment costs. The added power, extended range of capabilities and cost-saving benefits translate to greater efficiency for customers.

The NetWay8BT provides up to 90W power per port (480W total) for the most demanding Hi-PoE IEEE 802.3bt compliant devices, such as multi-sensor megapixel cameras or PoE lighting.

For devices demanding power up to 60W each, Altronix now offers the NetWay8GP which provides up to 60W of power across all 8 ports (480W total). The NetWay8GL provides 60W on any designated port up to 240W total across the unit's 8-ports.

The new NetWay 8-port Midspans features a 1U rack enclosure; 10/100/1000 Mbps data rates at distances up to 100m; and an integral battery charger for applications requiring backup.

The NetWay8GP and NetWay8GL also feature embedded Altronix LINQ™ Technology to monitor, control and report power and diagnostics from anywhere.

Altronix also debuted the NetWay XTG PoE+ Gigabit Ethernet Repeater, which extends data (video) up to 100m with a maximum possible range of up to 600m using multiple units.

Additionally, Altronix launched the

NetWay5B 5-Port Ethernet Switch which allows up to four IP devices to be connected to the headend using a single CAT6 Ethernet cable. Designed to be mounted in any Altronix enclosure, this new NetWay5B 5-Port Ethernet Switch greatly reduces installation costs by eliminating the need and expense of running dedicated cables for each individual deployed device. NetWay series products are backed by a lifetime warranty. SST

New Low-Cost Multi-Form Panic Solution Works With Any Device

The new Multi-Form Panic Solution from Maxxess Systems is able to work with any device, effectively lowering the cost of entry for proactive security while enabling total situational awareness for organisations. The innovator in security solutions launched the product at ISC West 2019.

A software-driven solution, Multi-Form Panic Solution can be configured to work with any smartphone, tablet, PC keyboard or wearable device. This allows organisations to easily create a panic notification system without having to purchase and deploy application-specific panic buttons and software.

Multi-Form Panic Solution can be deployed either as a standalone solution or integrated with any of Maxxess Systems' enterprise system management and control and communications platforms, as well as with numerous VMS and access platforms from third-party suppliers.

Maxxess Systems' software engineers were initially looking to develop a more efficient panic notification solution for another new product, the InSite Awareness and Response Coordination System. The team ended up creating a highly affordable solution that is equally effective as a standalone solution. SST

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

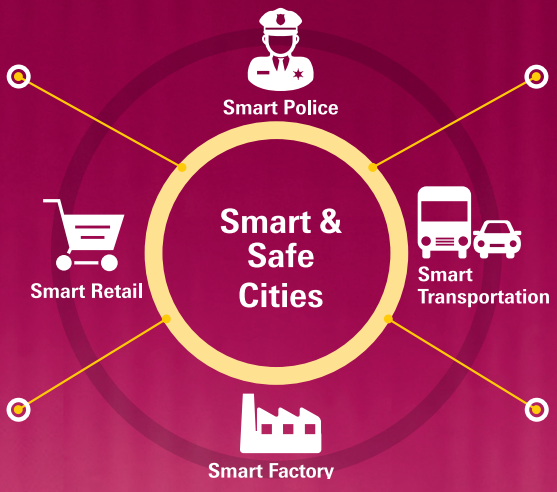
- International airports
- High-speed rails
- Motorways
- Sea ports
- Hospitals
- Tourism
- Industrial factories

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

Safeguarding Assets And Keys In A Smart Way

Morse Watchmans, a leader in key control and asset management systems, showcased its AssetWatcher and KeyWatcher Touch products at ISC West 2019 in April.

The two new key and asset management solutions protect important keys and physical assets for reduced downtime, fewer losses and improved accountability.

AssetWatcher is a flexible, scalable RFID-enabled locker system for safeguarding tools, mobile electronics and other valuable items. It can support more than 10,000 users on a single system and is configurable in three modes for flexible usage. The RFID technology allows users to easily track who is removing or replacing an asset, as well as when and where in the system the asset was taken from or placed.

Available in 10-, 22- and 34-locker configurations, each AssetWatcher locker is sized for small laptops, tablets, phones and other objects. Additional systems can be added as needed to expand the solution to support even more lockers. Each system is designed to be freestanding and can be mounted to the wall or the floor for convenience and stability.

KeyWatcher Touch is a key management system that features a 7" touchscreen with an easy-to-use interface and patented SmartKey system with KeyAnywhere technology to make it simple to withdraw and return a key securely to any key cabinet in an enterprise. Scheduled PDF reports are emailed

AssetWatcher

KeyWatcher Touch

to authorised recipients. Reports can also be accessed using the Morse Watchmans smartphone app. The system also enables security management to notify a user via email when a key becomes overdue.

Morse Watchmans also debuted KeyWatcher Fleet at ISC West 2019. KeyWatcher Fleet is the first key management platform designed with fleet managers in mind, with a key control system built on software designed specifically for fleet management.

A dashboard displays vehicle use, bookings and status. Vehicles can be assigned by lowest mileage, most fuel and priority. Drivers can be notified automatically via email or text if a specific vehicle is not available, while unique pin codes or optional card or fingerprint readers provide strong key and vehicle management. SST

Sentinel Retro PRX+12215 Named Best Intrusion Detection And Prevention Solution At ISC West 2019

HSI Sensing's Sentinel Retro PRX+12215 was named Best Intrusion Detection and Prevention Solution at the 2019 SIA New Product Showcase Awards. This flagship award show of ISC West recognises innovative security products, services and solutions.

The Sentinel Retro is designed as a drop-in replacement to simplify the upgrading of outdated technology and seeks to eliminate some of the most common issues that plague the industry, such as false alarms from shock and vibration, and alignment and mounting limitations.

Sentinel line of sensors are the most advanced high

security door contacts listed to UL 634 Level 2. Sentinel technology utilises Hall sensors and intelligent algorithms, making them resistant to physical, electrical and magnetic tampering. Advanced engineering has also eliminated alignment issues at install and the product can accommodate long-term door sagging. 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

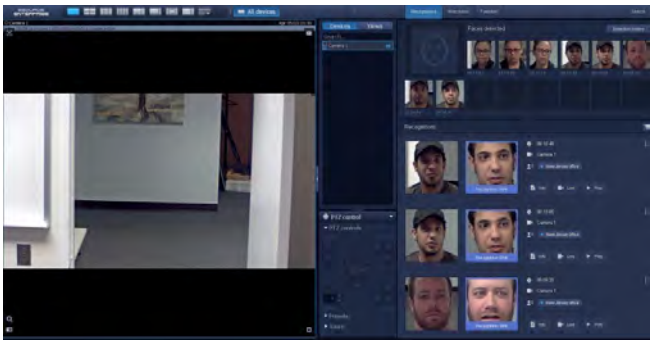
VIETFAIR

SecurOS FaceX Sets New Benchmarks In Accurate Facial Recognition

Intelligent Security Systems (ISS) has launched its new SecurOS FaceX facial recognition solution that is touted as setting a new benchmark for accuracy in facial recognition. It is superior in its ability to identify and match faces. Most notably FaceX resolves longstanding challenges for facial recognition related to camera viewing angles, facial expressions and diverse lighting conditions, providing for a far greater range of identity matches and authentication.

SecurOS FaceX compares captured images against databases of known individuals, or faces captured from video streams, expanding the use of facial recognition to search for individuals during unfolding events. Searches can also be conducted by specific facial features against multiple watchlists and a virtually unlimited database of facial images. SecurOS FaceX can clarify a database search based on specific face features such as age, gender and ethnicity, as well as by hair colour, the presence of facial hair, glasses, headwear and bald patches.

SecurOS FaceX also supports multi-factor authentication for implementation with access control systems. The new native analytics solution is built on the basis of ISS' recently enhanced SecurOS v.10 Video Management System (VMS) platform, embedding all of FaceX's functionality including



the ability to add and import files, perform searches and more.

"Our new SecurOS™ FaceX Facial Recognition Solution provides a significant leap in performance and capabilities for a wide range of surveillance and business intelligence applications. Its enhanced ability to accurately capture and identify individuals using profile images and facial characteristics greatly expands the range of applications for facial recognition across numerous surveillance and business intelligence applications," said Shawn Mather, Director of Sales for U.S. at ISS. SST

Smart Interlock Door Controllers Packed With Features

Dortronics, a provider of off-the-shelf and customised door control solutions, has launched a series of door controllers that is loaded with features. The 4800 Series Intelligent Interlock Controller accommodates up to five doors, including doors with automatic openers. It boasts adjustable timers for propped door time, panic release unlock time and unlock pause time for REX unlock time. Its features include 12 inputs for door status, request for access, interlock override and emergency unlock. Its 17 outputs control door locks (fail-safe or fail-secure), traffic lights and mirror door status with alarm outputs.

4800 Series Intelligent Interlock Controller raises the bar in versatility

Additional highlights include a watchdog circuit to monitor operation, LED input/output status indication and voltage spike/surge protection.

This extensive clutch of features provides installers with a higher degree of versatility to meet customers' specific needs. It also hands the installer complete control of all operating and configuration options without the need for complex software.

Said John Fitzpatrick, President of Dortronics Systems, Inc., "This provides installers and end users with an efficient and easy-to-use access control solution."

The 4800 Series is available as a controller board only or with a 4-amp Class 2 UL 294 power supply. SST

Shot Tracer Launches Outdoor Gunshot Detection Sensor

Shot Tracer Technologies has extended its gunshot detection solution to the outdoors.

The innovator in affordably priced gunshot detection solutions debuted its Hawk Outdoor Gunshot Detection Sensor at ISC West 2019. Hawk extends the detection capabilities and cost-effectiveness of Shot Tracer's gunshot detection solutions to exterior locations.

By automatically detecting and pushing notifications of gunshot activity from the instant an incident begins to unfold, Hawk empowers security personnel and first responders to best manage active shooter situations before a facility is breached.

Hawk is as easy to install as a smoke detector with analog and IP configurations available to integrate with virtually any security system available. Hawk integrates with security, alarm, surveillance and access systems via contact closure (Hawk AP) or wirelessly via IP integration (Hawk IP).

Upon detection of a gunshot, Hawk AP immediately sends a contact closure alert to the facility's alarm panel indicating whether it was a single or multiple gunshot event. Hawk IP sends alerts of detected gunshots' time, location and number of shots fired over Verizon (USA) or Vodafone (Global) wireless services to user-designated individuals including the local police and medical facilities. This eliminates the need for any additional external monitoring services. A PAN Wireless option is also available to pair Hawk IP sensors with other wireless sensors.

Shot Tracer Technologies first developed its Shot Tracer gunshot detection solution in 2010 in response to the shooting death of a Montana Highway Patrol officer. It delivers the highest accuracy and largest detection footprint per sensor available with

Shot Tracer Hawk™ Outdoor Gunshot Detection Sensor

critical data providing first responders with the information needed to protect people, property and assets.

Said Allan Overcast, CEO and President of Shot Tracer Technologies, "Every second counts in an active shooter situation and Hawk's ability to detect gunshots from outdoor locations in real-time allows security and personnel to react to unfolding active shooter situations before an assailant enters a facility."

Shot Tracer Hawk Outdoor Gunshot Detection Sensor will be available June 1, 2019. SST

Video Assurance Service Helps Firms Manage Security Videos

Many small and medium-sized businesses do not have dedicated staff to manage their video systems. This often results in failures going unnoticed. This gives rise to gaps in the video record, also called 'missing video evidence'. Unfortunately this missing video evidence often isn't discovered until it is too late, when it is needed for investigation or for compliance purposes.

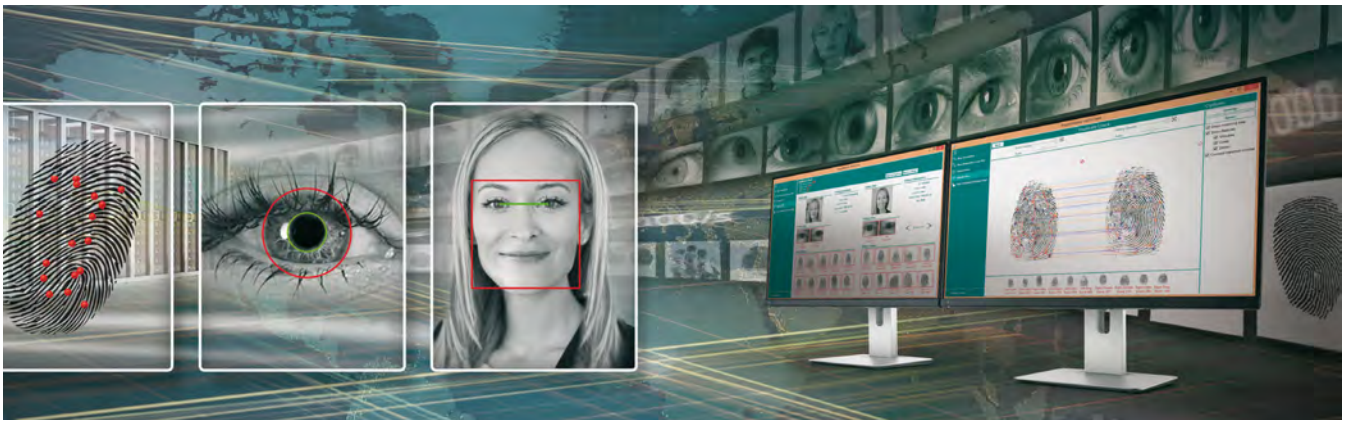
Viakoo, the security industry's only provider of service assurance and IoT applications management solutions for physical security systems, offers the answer to this with its new Video Assurance Service.

With Video Assurance Service, Viakoo will provide the oversight, automatic problem detection and continuous automated diagnostics and offer customers recommendations on how to fix it. Viakoo teams with partners to resolve the problem either remotely or onsite. Customers receive a weekly summary report. The service is currently offered by Viakoo in partnership with Stanley Security and PSA Security Network.

A key customer segment is very small and medium-sized firms. Video Assurance Service equips small and medium-sized end users with the ability to identify security risks and vulnerabilities in real time and solve those risks in a quick and efficient manner while mitigating future weaknesses.

The service is also targeted at integrators looking to deliver managed services and build recurring monthly revenue. SST

Neurotechnology's Multi-Biometric Solutions Now Feature Top-Ranked Palm Print Recognition Technology

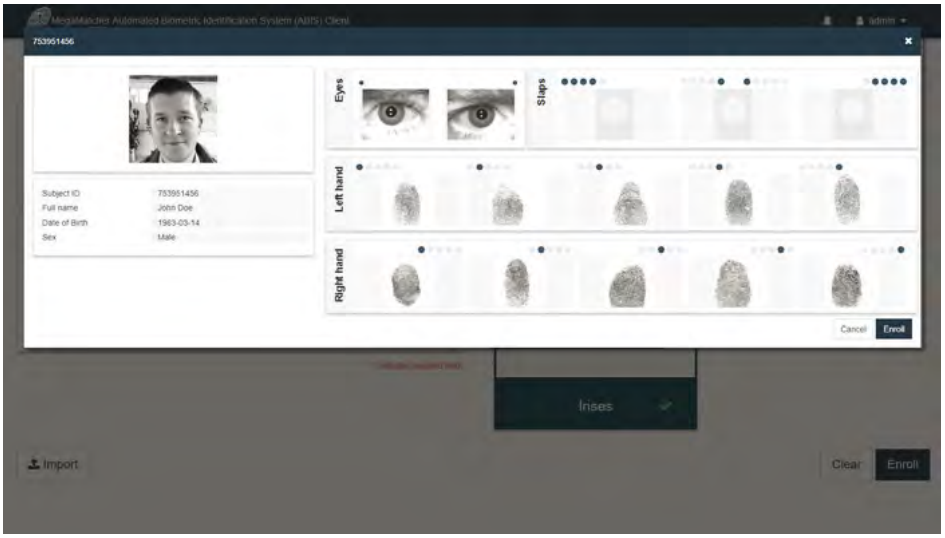


MegaMatcher

Neurotechnology's latest palm print recognition technology is the fastest and most accurate on the market, and it is now included in the MegaMatcher Accelerator and MegaMatcher Automated Biometric Identification System (ABIS).

Neurotechnology is a developer of high-precision algorithms and software based on deep neural networks and other AI-related technologies. Its MegaMatcher products and solutions are currently used for a wide range of security, civil and forensics projects.

The company's latest palm print algorithm achieved top rankings for speed and accuracy in a recent FVC-onGoing evaluation. It was ranked the most accurate for both full and partial palm prints.



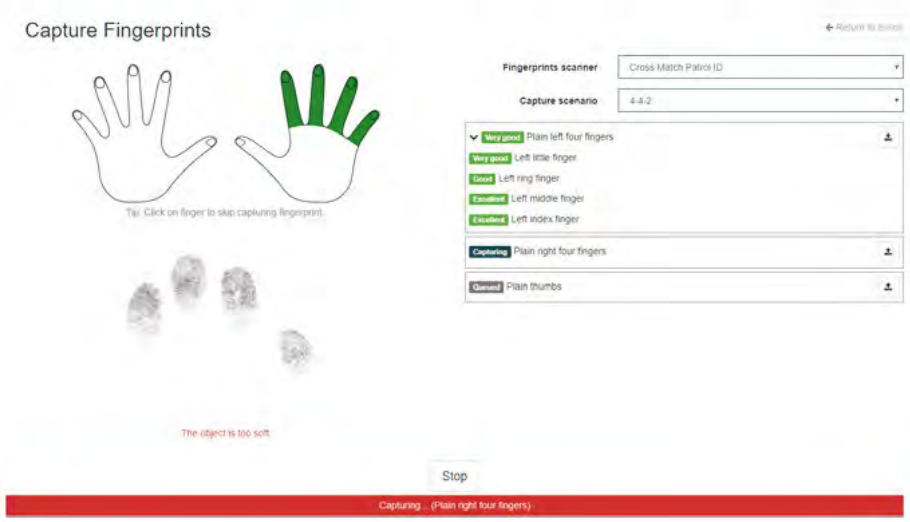
MegaMatcher Accelerator is a combined software and hardware solution that provides high-speed, high-volume biometric identification for national scale projects. The MegaMatcher Accelerator Extended edition can manage up to 4,000,000 palm prints on a single server with a matching speed of 2,000,000 palm prints per second. The palm print recognition feature can be used alone or in any combination with fingerprint, face and iris biometric modalities.

continued on page 19

The updated MegaMatcher Accelerator opens new possibilities for large scale multi-biometric systems with seamless integration of all supported biometrics, namely fingerprint, face, iris and palm print.

MegaMatcher ABIS is a turnkey biometric solution that includes all of the algorithms and software necessary for the deployment of large-scale multi-biometric projects.

A free 30-day trial is available. SST



Sielox Enhances Access Control Platform

Sielox LLC has added new functions to its Pinnacle™ v.10.4 Access Control Platform that enhance the implementation and maintenance of Wi-Fi locks on Sielox access control platforms.

Pinnacle v.10.4 now provides seamless integration with Allegion Schlage NDE and LE wireless locks so they can easily be incorporated as part of a facility's overall access control system using existing Wi-Fi infrastructure. The Pinnacle Schlage Wi-Fi integration provides access to the wireless locks' features, enabling advanced door management capabilities along with credential management, detailed audit reports and customisable screen layouts. With this integration, users are able to control an unlimited number of Allegion Schlage NDE and LE wireless locks, manage cardholder records, create access groups and define holiday schedules.

Allegion Schlage wireless locks can also now receive firmware updates through Sielox's 1700 controller using Allegion ONR technology, which will save integrators tremendous time and money when upgrading and maintaining layered security systems.

Sielox has also added a new Transport Layer Security (TLS 1.2) enhancement to Pinnacle v.10.4. TLS and its predecessor Secure Sockets Layer (SSL) for improved network security. TLS/SSL operates by establishing an encrypted communication path between two applications, 'wrapping' the entire application protocol inside the secure link. This

provides complete privacy for the entire transaction so that sensitive information is protected from unauthorised access while in transit.

Another update to Pinnacle v.10 is Lightweight Directory Access Protocol, a licensed service that can be installed on the same server as Pinnacle. The feature simplifies administration by assigning roles to users with permissions.

All these new features boost the versatility and cost efficiency of Pinnacle for myriad access control applications.

Pinnacle 10.4 will be released in Q2 2019. SST

All-In-One Drone Service For Autonomous Security, Safety And Inspection Missions

Leading provider of on-site autonomous drone solutions for critical infrastructures and industrial sites Percepto has launched an all-in-one aerial solution for autonomous security, safety and inspection missions in Australia.

Percepto is a recipient of the Frost & Sullivan Global Enabling Technology Leadership Award.

The Percepto Sparrow drones deliver fully autonomous real-time human/vehicle detection and tracking, thermal inspection, gas/oil leak detection, 2D mapping, 3D modelling and fence and property patrols - all without need for a pilot or an on-site operator. The solution delivers value across a diverse range of industrial and enterprise applications in sectors including mining, oil and gas, renewable energy, utilities and port and sea terminals.

The solution is suited to any large-scale enterprises looking to improve security, increase productivity and reduce safety risks and operational costs. Organisations using the Percepto solution are better aware of events taking place, allowing them to be proactive and more efficient in addressing risks and operational needs.

The drones are equipped with high-definition thermal cameras to enable day and night operation. They can perform in hostile weather conditions including rain, snow and dust. When deployed in the field they take off on demand or at scheduled times and navigate pre-defined routes.

Once the mission has been completed the Sparrow returns to its base station - a highly secure enclosed weatherproof box - where automated post flight checks and fast battery charging are completed, ensuring the drone is primed for the next flight. The system is the only 'drone-in-a-box' solution that is powered by computer vision and AI, and that provides communications over LTE. SST

Ultrasonic Speaker That Releases Focused Beams Of Sound

Neurotechnology has launched an ultrasonic directional speaker that focuses and constrains sound to a narrow beam for tens of metres. Listeners in the path of the beam are immersed in the music or speech projected by the speaker but just steps away no sound can be heard.

Neurotechnology is a developer of high-precision algorithms and software based on deep neural networks and other AI-related technologies.

Built on Neurotechnology's patent-pending ultrasonic transducer technology, the Focusonics speaker is ideal for situations where sound reproduction needs to be localised to a certain area while quiet is maintained elsewhere. These scenarios include targeted public address and warning systems, promotions in retail showrooms or trade shows and displays in art galleries or museums.

continued on page 21

Focusonics can be combined with AI-based computer vision applications to create custom public security and safety solutions and automated warning systems. The beam of the Focusonics speaker attenuates very little with distance and can be used to attract the attention of people from a significant interval away. For example, a video camera and Focusonics speaker together can be used to detect a person entering a doorway or crossing a line, determine that person's attributes such as age, sex and even mood, and issue a message or warning. It can also be used to inform people at security checkpoints about what to remove from their luggage or transmit warning messages specifically to people who cross the safety line on a train platform.

Said Dr. Osvaldas Putkis, research engineer and project lead at Neurotechnology, "As the ultrasonic waves travel through air they de-modulate and sound can be heard, however the diffraction of ultrasonic waves is much smaller than audio frequency waves, so the sound coming from the Focusonics speaker is constrained to a narrow beam. To the listener, it feels as if the sound is generated in the air just in front of you, creating a feeling of immersion and surround sound." SST

Focusonics Model A Directional Speaker

Synopsys Named Leader By Gartner For Application Security Testing For 3rd Year

For the third year running, Synopsys has been recognised as a Leader by Gartner Magic Quadrant for application security testing (AST).

In the report, Gartner evaluated 11 application security testing vendors based on their completeness of vision and ability to execute. Synopsys was placed highest for its ability to execute and furthest to the right for completeness of vision.

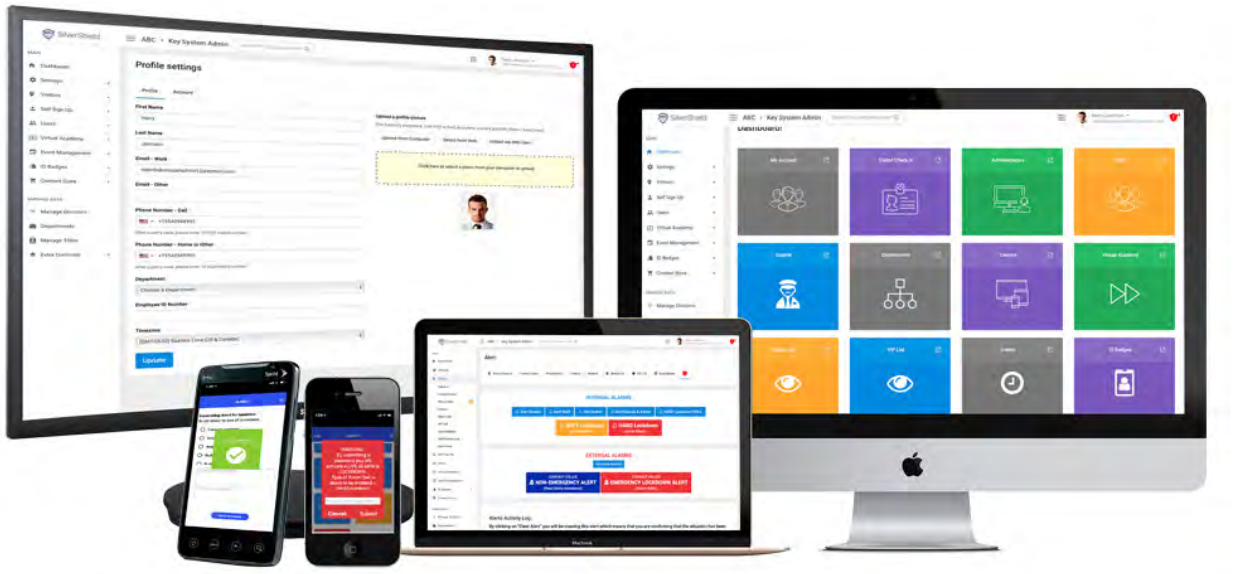
Today the pressure to launch apps to market is insane, and companies - including governments - often find themselves in the hot seat of cybersecurity vulnerabilities, data theft, ransomware and malware due to shoddy coding, said Synopsys. That is why Synopsys has adopted the shift left paradigm, where security is written into software from the get-go, rather than trying to patch it only when errors and hacks occur.

"AST solutions must be fast, automated and integrated into the development pipeline in order to effectively manage application security risk in modern DevOps environments," said Andreas Kuehlmann, co-general manager of the Synopsys Software Integrity Group.

"At the same time, they need to produce high-fidelity results that facilitate prioritised and efficient remediation efforts to avoid unwanted friction with developers. We believe Gartner's continued recognition of Synopsys as a Leader in application security testing validates our strategy and ability to address these customer needs."

Over the past year, Synopsys has introduced several new offerings and enhancements to its software security portfolio. They include the Polaris Software Integrity Platform, a cloud-based integrated solution that enables security and development teams to build secure software faster. It also introduced the Code Sight IDE plugin that extends the power of Synopsys' solutions to the developers' native work environment, enabling them to easily find and fix security vulnerabilities in their code as they write. SST

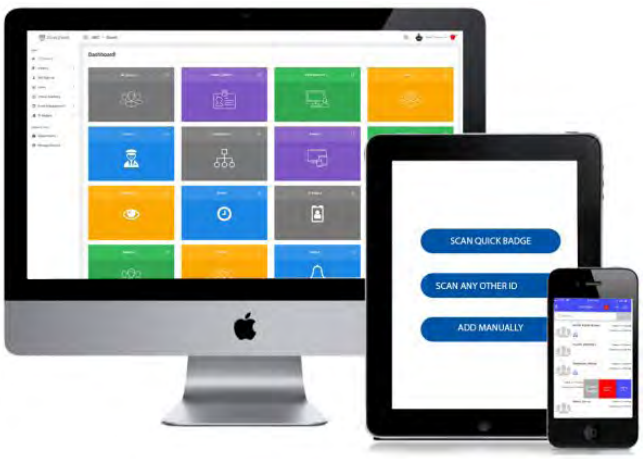
SilverShield Debuts Self-Service Kiosk For Unmanned Visitor Registration At ISC West 2019



Many business owners struggle with the challenge of securing their facilities while containing the cost of manned security personnel. One answer to this is unmanned visitor registration kiosks.

In April at ISC West 2019, provider of cloud-based, multi-platform solutions SilverShield Safety & Information Systems offered business owners an answer with its version of the unmanned visitor registration kiosk.

The SilverShield Kiosk is integrated with the SilverShield Visitor and Incident Management System so that organisations are able to screen and check in visitors and guests without an officer present.



The kiosk allows visitors to register themselves using a Mac or PC computer, iOS or Android device. The process is fast and easy: users enter their credentials manually or scan their valid IDs or SilverShield Quick Badge. Once a visitor's details are entered, the SilverShield Kiosk notifies a Kiosk Monitor (this may be a system administrator or security guard) that a visitor has completed check-in. The Kiosk Monitor can then decide to allow access or deny access.

If a visitor's details match those on any watchlist or sex offender registry, the Kiosk Monitor may send silent alert notifications to any stakeholders the organisation chooses. If the visitor denied access becomes a threat, the Kiosk Monitor can initiate additional internal or external alarms they feel are needed such as Alert Security or Hard Lockdown.

"Our Self-Service Kiosk helps organisations secure all of their entry points so they know who is on their premises at all times, even those entry points that are unmanned," said Robin Baker, CTO, SilverShield. "Even a single uncontrolled entrance could otherwise compromise the safety of the facility."

"The SilverShield Self-Service Kiosk ensures that all visitors are correctly checked in, screened and badged," said Baker. "It's one more way that SilverShield Systems helps keep your facility safe and secure." SST

Breakthrough By NUS-Singtel Cyber Security Lab Fast-Tracks Next-Generation Cybersecurity Development

Researchers from the National University of Singapore (NUS) and Singtel have advanced cybersecurity with a breakthrough technique in quantum key distribution.

Quantum key distribution is a protocol that transmits light particles, or photons, over a network, so that two communicating parties can agree on and generate an encryption key to establish a secure communication channel. The researchers succeeded in coordinating the travel of a pair of photons (one for each party) through different fibre network paths, controlling precisely the photons' arrival times. Without this technique, the photons may get out of sequence, making it difficult for both parties to agree on an encryption key.

Quantum key distribution is resistant to all types of computational hacks, including next-generation quantum computing threats. Any attempt to eavesdrop will increase the error rate of the photon sequence. This alerts the two communicating parties to an intrusion so that they can abort the session and start a new one.

The breakthrough was demonstrated over Singtel's fibre network, paving the way for wider Quantum key distribution adoption and future commercialisation. The technology opens up many exciting possibilities for users who require strong and long-term security for their communication.

The researchers are now working on developing the findings for actual use cases where quantum-resistant secure communication is needed to provide long-term security, such as government, military and bank services.

In the future, quantum key distribution hardware could even be integrated with the internet to develop security solutions for online payment services such as internet banking and online shopping. As the smooth photon pair navigation enables high-precision clock synchronisation, this discovery can also be deployed in time-critical operations such as real-time big data analytics and financial trading.

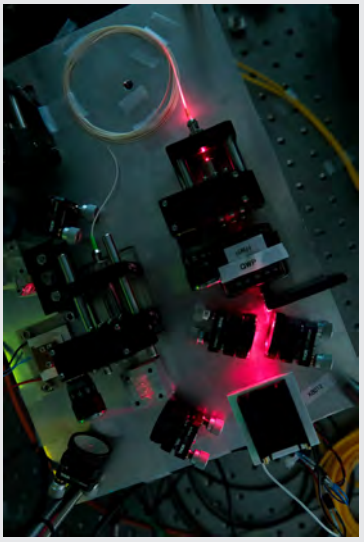
"The breakthrough achieved by the NUS-Singtel Cyber Security R&D Lab not only strengthens our defences in a new cyber reality where threats are becoming more sophisticated, it also positions Singapore as a hub for global QKD research," said Mr Bill Chang, CEO, Group Enterprise at Singtel.

The team plans to provide keys across live fibre by the end of this year. Such keys could in principle be used to update AES encryrptors every few minutes. An example of where AES encryptors can be used is entreprise data security where the communications is secured through a Hardware Security Module.

Conducted in Singapore, the project is driven by the NUS-Singtel Cyber Security Research & Development Laboratory. The lab is a public-private partnership supported by the National Research Foundation, Prime Minister's Office, Singapore, that was set up in October 2016 to develop cyber security capabilities and solutions. The researchers published their findings in Applied Physics Letters journal in April. SST

(From left) Senior Research Fellow Dr. James Grieve of the Centre for Quantum Technologies at NUS and Dr. Amelia Tan, Principal Investigator of the project and Senior R&D Engineer of Trustwave, Singtel's cyber security subsidiary.
Image credit: National University of Singapore

Dr. Jia Xu (pictured left), R&D manager from Trustwave, and Soe Moe Thar (pictured right), a Research Assistant, at the Centre for Quantum Technologies at NUS with some of the hardware being developed for advancing quantum technology at the NUS-Singtel Cyber Security R&D Lab



A device developed in the NUS-Singtel Cyber Security R&D Lab that creates photons connected by the quantum property of entanglement

World's First Palm Vein Authentication System Deployed At Korean Airports

Passengers travelling on domestic flights in Korea can now verify their identity just by holding out a hand, boosting travellers' convenience and reducing congestion.

Since March 27, the Korea Airports Corporation has deployed a palm vein authentication system at all 14 domestic airports under its jurisdiction to ease congestion. The palm vein authentication from the Fujitsu Group has a track record of use by banks in their ATMs and corporations to control access to PCs.

After checking in, users who have registered their palm vein patterns in advance can confirm their identity instantly by just holding out a hand and ticket over the gate. They will not have to show their citizen ID card, which, in the past, was necessary to confirm the passenger's identity.

This automating of the identification process increases the accuracy of passenger identification and significantly shortens the time required for the process.

The domestic airports under KAC's jurisdiction (a total of 14 airports) are currently used by about 32 million people per year. Korean citizens over the age of 14 travelling on domestic flights must have their identity checked before passing through boarding security. Previously this was done on-site by showing a citizen ID card to security personnel. Because visually confirming a passenger's identity takes time, this process could lead to congestion in the airports. In addition, passengers who had not brought their citizen ID cards were not able to board their flights, which mars customer experience at the airports.

For these reasons, KAC decided to deploy a personal identification system based on palm vein authentication. The system first began operation on December 28 2018, and to date it has been used over one million times, with 160,000 individuals having already registered their palm vein patterns.

How It Works

Travellers register in advance at registration devices installed in airports to use the palm vein authentication system. The registration will link their palm vein pattern with their citizen ID number, name and phone number. After they have registered, travellers simply need to scan a barcode on their ticket and then confirm their identity by holding out their hand at the newly installed identity confirmation gates.

Features Of The Newly Deployed System

Delivers greater security with high accurate identification rate. The identification process is highly accurate as it identifies individuals with biometric data. It is also sanitary, due to its contactless operation.

Greater convenience with smooth personal identification process. Having their identification verified instantly through the simple action of just holding out one's hand over the gate elevates the boarding experience for passengers. It also means they can board even if they had forgotten to bring their citizen ID card.

Reduction of congestion within airports. By automating the process of confirming passenger identities, congestion is significantly reduced.

The Fujitsu Group is currently in discussions with KAC to expand palm vein authentication to self-service check-in systems and self-boarding gates, to further improve airport services. SST

Dahua's New Video Recorder Features SMD Plus For Tenfold Computing Power

Leading video-centric smart IoT solution and service provider Dahua Technology has launched a new video recorder that incorporates SMD Plus to ramp up computing power.

The new XVR series, XVR5000-I/XVR7000-4KL-I, features full-channel SMD Plus to allow customers to benefit fully from AI technology. Based on Dahua-patented HDCVI technology, the new XVR series integrates SMD Plus, perimeter protection and active defence to secure properties while saving manpower.

SMD Plus: Highly Accurate Smart Motion Detection

An upgrade from the original SMD technology, the new SMD Plus adopts independent AI smart chip loaded with new deep-learning algorithm for a tenfold improvement in computing power.

SMD Plus can recognise moving objects and identify humans and vehicles. This means no more false alarms caused by tree branches, insects, shadows, wind or other environmental factors. Meanwhile, users are allowed to select people or vehicles for playback, thus greatly saving target search time. With this, both false alarm rates and human surveillance costs are slashed.

In addition, through the added real-time tracking box, users can clearly see the detected target on the screen for visualised alarm management.

One Device Upgrade To Enjoy Full-Channel AI Surveillance

Most perimeter protection products support two to four channels. Dahua SMD plus XVRs support up to 16 channels and is suitable for indoor corridors, outdoor park entrances and many other applications. HDCVI users just need to replace a cost-effective backend product to enjoy HD-over-Coax with advanced AI performance.

Active Deterrence To Prevent Violations And Crimes

When paired with Dahua Active Deterrence Camera, XVR5000-I/XVR7000-4KL-I can repel any intruder detected by SMD Plus with white light and siren, actively defending the property while saving manpower.

Alert messages can also be remotely sent to the DMSS App installed on the users' mobile phones to keep them updated on abnormal situations anytime anywhere. This intelligent function meets the safety requirements of all kinds of properties vulnerable to attacks, including shops, villas and warehouses. SST

Dahua Becomes Member Of Forum Of Incident Response And Security Teams

The Dahua Product Security Incident Response Team (Dahua PSIRT) has joined Forum of Incident Response and Security Teams (FIRST).

FIRST is an international organisation composed of a number of Computer Emergency Response Teams (CERT) around the world. Focusing on the cooperative handling and risk prevention of computer network security incidents, it brings together more than 400 members from 90 countries. The members include Intel, Apple, Cisco, IBM, Oracle and Microsoft as well as organisations such as CERT/CC, CNCERT/CC, us-cert, cert-eu and AusCERT.

As a member, Dahua PSIRT will be able to offer customers efficient security services and technical support in the areas of vulnerability determination, vulnerability response and security event response as well as in the outbreak of security events such as virus and worm infections. SST

China Presents World's First 5G Smart Hotel

InterContinental Shenzhen, Shenzhen Telecom and Huawei have signed a strategic cooperation agreement to create the world's first 5G smart hotel.

InterContinental Shenzhen is the first Spanish inspired luxury business hotel in China. The hotel has won numerous international and domestic hotel industry awards for its creativity, attentiveness and personalised service.

At the hotel, the three partners will introduce the hotel industry's first end-to-end 5G network with integrated terminals and cloud applications, to provide guests with the ultimate innovative luxury experience.

Shenzhen Telecom is deploying Huawei's 5G network equipment in the InterContinental Shenzhen to achieve continuous indoor and outdoor 5G coverage, which will serve as the platform for a new generation of hotel services. Guests will experience innovative 5G hotel applications through 5G smartphones and customer premises equipment (CPE) terminals, including 5G welcome robots, 5G cloud computing terminals, 5G cloud games and 5G cloud virtual reality rowing machines, providing business travellers with a convenient and efficient working environment, and leisure travellers with a high-end, immersive entertainment experience.

In the hotel lobby, guests can access the 5G network through CPEs or their smartphones to experience high-speed 5G downloads and uploads. Service efficiency is improved with 5G intelligent robots that provide services including guest information, destination guidance and goods delivery.

The presidential suites covered by the new network will offer 5G hotel services such as cloud VR rowing machines, cloud games and 4K movies.

Golden Sun, General Manager of Shenzhen OCT Hotel Development Co., Ltd said, "Guests expect new things and new experiences. The joint venture with Shenzhen Telecom and

Huawei has brought more possibilities to the hotel. Riding on the advanced technology, we can imagine our future and fly with it freely." SST

With Smart Buildings, New Possibilities Emerge Every Day

We all spend a huge part of each day in buildings but they are largely inefficiently ran. Most buildings operate on multiple systems for lighting, heating and security, and all these systems are administered independently of each other.

By and large, buildings waste energy, are not optimal in space usage and are expensive to run.

Furthermore, with so many assets to manage, extensive technologies, increasingly sophisticated system landscapes and complex data, facility managers are inundated with information and often feel overwhelmed.

> "WE FIND NEW POSSIBILITIES EMERGING EVERY DAY."
>
> – Michael Goh, Director of Sales ASEAN, Security and Safety Systems for Robert Bosch (SEA) Building Technology division

Humans And Buildings: Connected To Work Together

For leading smart building solution provider Bosch, the answer is obvious: create connected buildings.

With its smart building solutions, Bosch seeks to connect buildings so they can interact with humans. The goal: to deliver easier-to-manage buildings that perform better while providing greater energy.

"New possibilities emerge every day," said Michael Goh, Director of Sales ASEAN, Security and Safety Systems for Robert Bosch (SEA) Building Technology division. "Smart buildings are the way forward because they improve manpower efficiency, provide real-time sensing and feedback, help reduce operational costs through preventive maintenance and enable many value-added services and applications, many of which are still in development as this is a relatively new field."

Bosch's wide portfolio of products for buildings ranges from connected home appliances, IoT sensors, fire detection systems with remote service, video surveillance with intelligent analytics, connected thermotechnology solutions and more. The smart building offerings go beyond hardware to include the Connected Building Services software and Bosch IoT Cloud.

Insights That Add Value

Smart buildings collect data from these operational systems and independent sensors to drive insights that add value beyond ensuring security and facilitating access.

For example, by fusing data collected from a video surveillance/video analytic system, access control system and building management systems, building owners can find key insights and trends pertaining to energy usage in relation to human traffic for a particular space in the building.

By supplying data on buildings and their technology, Bosch's solutions for commercial buildings will help facility managers and owners to always make the right decision.

SECURITY

Video Systems

Access Control Systems

Intrusion Alarm Systems

SAFETY

Fire Alarm Systems

Public Address

COMMUNICATIONS

Conference & Discussion

Commercial Audio

Integrated Solutions for Commercial Buildings

BUILDING MANAGEMENT & APPLICATIONS

Management Software

Cloud-based Services

Professional Services

IoT solutions for buildings, such as Bosch Software Innovations' Space Management Service, provide this data. This cloud-based service collects and processes information from building sensors and devices in near real time and delivers it to apps or online dashboards.

For instance, by deploying Bosch's smart sensors and video analytics in buildings, facility managers could better understand how people utilise space. With this information, they could analyse the space usage in the past and forecast future usage based on this historical data. This leads to the optimisation of energy consumption through the smart manipulation of lights and air-conditioning systems.

Furthermore health and status data collected from the individual cameras and access controllers over time can potentially uncover insights into why devices in a particular area break down more than usual. These insights can then be utilised in meaningful ways such as determining optimal servicing and maintenance schedule for the devices.

Bosch Software Innovations solutions also offer another huge benefit: Bosch's Connected Building Services provide a repository of data; a data lake from which data is analysed and various applications could be built upon.

Take for instance Bosch's elevator monitor solution. Alerts can be created for predictive maintenance before a fault occurs. Building owners and managers will also receive targeted, precise information about what areas require more attention. Meanwhile Bosch's energy monitoring solutions help track asset usage where maintenance schedules could be better planned even before the customer asks for it.

What The Connected Building Can Do

This is what Bosch's Connected Building solutions can do:

Elevator Monitoring And Management
Every three days, elevators carry the equivalent of the entire planet's population. Building owners and facility management companies want to reduce elevator downtime, but the lack of insight into operating data and high maintenance costs impedes their efforts.

Bosch's Elevator Manager improves operational transparency, responsiveness and efficiency by tracking anomalies and maintenance lapses centrally. It monitors elevator status, notifies support staff of critical events and, if necessary, escalates events to the attention of maintenance personnel. It monitors the duration of preventive maintenance checks, tracks their lapses, and compares elevator performance before and after maintenance.

Optimised maintenance schedules and instant notifications of critical events reduce downtime to a minimum while centralised tracking of operational anomalies and maintenance lapses ensures higher safety standards.

Bosch's solution provides an independent source of monitoring, as it can be deployed on elevators of any brand and model. Any older, existing non-connected elevators can be easily retrofitted with Bosch's sensors and connected to the system.

Bosch's Elevator Manager solution is already deployed in several hundreds of elevators in Singapore and their number is rapidly expanding.

Security Management
In smart buildings, video, access control intrusion and fire and public address systems for evacuation can all be integrated into one seamless system.

With Bosch's intelligent video analytics, guards can be alerted the moment something happens so that immediate action can be taken. Video-based fire and smoke detecting allows building owners and operators to quickly address any fire shortly after it happens.

Facial recognition access control helps to provide an added layer of security and prevents intruders from using someone else's access card as well as helps to spot tailgating.

Bosch's smart building solutions also up the efficiency of security operations. For example, forensic search features means that security personnel no longer need to look through hours of footage to identify when an incident of interest occurred; it now takes just seconds.

Better Cost And Space Management
Bosch's smart building solutions allow facility managers to design smart, connected environments at the workplace by accessing the latest data on their buildings from anywhere, at any time. This allows them to pinpoint malfunctions before substantial damage can occur, which will lead to cost savings. It also allows them to best utilise space at any time.

Air Quality Monitoring
Bosch's Smart Building solutions measure and monitor a range of air quality parameters to ensure healthy living and working environments.

A Future Filled With Connected, Attractive, Sustainable Buildings

"Bosch is transforming the buildings of tomorrow into connected, attractive, sustainable and effective spaces by offering building owners and facility managers connected solutions and devices. The possibilities are endless and at Bosch, we are truly excited about what lies ahead," pronounced Michael Goh. SST

SMART BUILDINGS: Our Connected, Integrated Future

►► **By Jared See,**
Technology Leader (Singapore), Global Technology Solutions, Cushman & Wakefield

Technology continues to redefine the world around us. And one of the ways technology is revolutionising our daily life is the way it is used in smart buildings to transform the landscape of building management.

But what exactly is a smart building?

A smart building delivers useful, integrated and smart services that make occupants productive at the lowest cost and with the least environmental impact over the building's life cycle. Fundamentally, smart buildings utilise technology to enable the convergence of siloed systems and processes into an integrated workplace management and operations framework.

Smart buildings are buildings that:

- Are equipped with smart networked sensors, meters, materials and devices
- Use automated processes to control, monitor and manage building assets and services
- Are linked with an energy and sustainability management programme
- Are connected to a network of intelligent systems, infrastructure and technology platforms

This new breed of buildings leverages information technology for real-time data exchange and system interoperability, empowering occupants with visibility and actionable insights through unified information generated by a platform of Internet of Things (IoT), Artificial Intelligence (AI), machine learning and analytics technologies. In short, smart buildings ramp up efficiency and enable exciting new possibilities.

Smart buildings bring together a wide spectrum of technology and business processes partners to deliver next generation, end-to-end solutions that leverage respective core

capabilities across the value chain. One of the significant trends is the growing partnership between IoT, business improvement and energy and facilities management domain experts through a scalable and open architecture as well as a redefined structure of processes. An example of this is the Cushman & Wakefield's Experience Per Square Feet programme.

Driving The Uptake

Building owners are always striving for stronger bottom lines. Facility managers constantly seek to increase efficiency of operations. Occupants want control of their work environment and greater comfort. By harnessing integrated workplace management solutions, smart buildings deliver benefits for all three parties, including productivity gains, increased staff performance, optimised space utilisation and occupant satisfaction.

These compelling benefits are driving the increasing adoption of smart buildings. Navigant Research estimates that the smart building market will generate global revenue of US$8.5 billion in 2020, up from US$4.7 billion in 2016.

Specifically, smart buildings deliver five core benefits:

- Integrated workplace and well-being management solutions that drive productivity, performance and longevity
- Energy and sustainability solutions for eco-friendly carbon footprint impact and compliance
- Increased efficiency via automation for workstream optimisation and cost saving
- Predictive maintenance capability for effective operation and better asset management
- Best practice and agile processes for converting reactive activities into smart services

Automation And Integration

Today's building capabilities include a certain level of process automation and system integration. Building Management Systems (BMS) and Building Automation Systems (BAS) are traditionally the underlying foundations for monitoring, controlling and managing the overall core building functionalities and services such as lighting, heating, ventilation and air conditioning.

Now, however, with Internet of Things (IoT), buildings can leverage open protocol standards to exchange and consolidate information between IoT technology and Industrial Control System (ICS) platforms. Through this they can derive AI-generated value-added insights to assist in decision making.

Facilities managers have been diving into predictive maintenance capabilities to anticipate failures, take corrective actions, make replacements, or plan ahead of scheduled maintenance. For example, predictive maintenance employs machine learning modelling to achieve greater accuracy. This leads to cost savings and optimising of scheduled maintenance.

Smart Building Technology Fundamentals

From a technological perspective, a smart building platform consists of three fundamental elements:

- Application of infrastructure and technology capabilities
- Transformation of monitoring, control and maintenance processes
- Adoption of security assessment and enablement

Every space, floor and workplace of a smart building must be strategically planned, designed and integrated to meet the core needs of operational efficiency and cost saving.

Deployment And Operation

The processes for operating the smart building requires transformed procedures as well as best practices to be adopted by every building resource. This ensures effective execution of workflows.

Well-deployed technology and a connected platform results in an integrated solution for the delivery of optimised resources through automatic alerts, self-recovery, auto-resource-assignment, reduction of waste and downtime, eco-sustainability, streamlined maintenance, and ultimately, improved productivity.

A Centralised or Remote Operations Centre (ROC) is one of the outcomes of processes improvement. Through the ROC, traditional processes are transformed and redefined to optimise the operations of buildings and maintenance, providing monitoring, control and mitigates risks across various geographical sites through a connected platform as well as swift response from a mix of stationed and mobile dispatch team.

AI technology based within the ROC, for instance AI-based chatbots, have transformed the conventional way that facilities maintenance teams work with call centre staff, by increasing the productivity of call handling (machine vs. man) and the automation of schedule management. Further benefits of ROC include real-time fault reporting, incident prevention, efficient operations, effective cost in resources and predictive alerts.

Managing And Securing The Site

In smart buildings, facilities engineers can make use of tools such as digital twin technology or Building Information Management (BIM) viewer applications to efficiently manage the assets and facility operations. This includes simulation analysis prior to inspection, plan-ahead of trips, and ease of documentation access during field works. Integrated with Computerised Maintenance Management System (CMMS), a BIM viewer application conveniently enables field service staff to handle the work order management.

AI TECHNOLOGY BASED WITHIN THE ROC, FOR INSTANCE AI-BASED CHATBOTS, HAVE TRANSFORMED THE CONVENTIONAL WAY THAT FACILITIES MAINTENANCE TEAMS WORK WITH CALL CENTRE STAFF, BY INCREASING THE PRODUCTIVITY OF CALL HANDLING (MACHINE VS. MAN) AND THE AUTOMATION OF SCHEDULE MANAGEMENT.

Security components of smart buildings fall into the categories of physical, hardware and cybersecurity measures. These include mobile and stationed security forces, intelligent surveillance cameras, closed-circuit television (CCTV) and alarms, biometric systems such as facial recognition technology, detection sensors, advanced locking systems and back-end AI-based platforms that can flag threats.

These tools can provide alerts or alarm trigger, plus protection and shields within a well-defined security response procedure. By further certifying and complying with information security standards like ISO27000/27001, intelligent buildings can measure up to stakeholders' security expectation.

No matter how well equipped the buildings are, smart buildings must always still incorporate an 'always be prepared for the unexpected' contingency action plan as part of the organisation's business continuity plan. SST

Cushman & Wakefield is a leading global real estate services firm with 400 offices in 70 countries.

Smart Buildings: What 'Smart' Really Means

▸▸ By Dr. Patrick Lecomte,
Associate Professor in Real Estate at Henley Business School, University of Reading (Malaysia)

REAL ESTATE, a mostly passive spectator of technological changes for years, is being disrupted at last under the unrelenting pressure of smart technologies applied to all aspects of the built environment (construction, valuation, transaction, operation, management).

Disruption in real estate comes from two concomitant changes. Firstly, the property sector itself has moved at the epicentre of a technology revolution with the emergence of property technology (proptech), a broad term covering the wide range of applications of digital technology to the property sector. Secondly, digital innovations are revolutionising the way urban environments and buildings function and interact, enabling new lifestyles favoured by millennials (such as co-working) and giving rise to a new type of building called 'smart buildings'.

Smart buildings are essential components of any smart city project. They are an instrumental part of smart energy grids and serve as real-time adaptive platforms collecting data to feed increasingly sophisticated analytics. In the process, they foster productivity, efficiency and overall well-being of their occupants. There is however one problem that needs to be urgently addressed if we want the promises of the digital revolution to fully materialise in the built environment: smart buildings still lack common standards and metrics to quantify their value and contribution to urban environments' overall smartness.

Need For Smart Building Metrics And Certification

Similar to green buildings' widely used LEED (Leadership in Energy and Environmental Design) certification, smart buildings have to come with ad hoc norms and standards to certify their performances and guide commercial real estate players. Attempts to design evaluation frameworks and smartness scores have so far been hindered by the lack of consensus among multiple and diverse stakeholders (private sector, public authorities, technology companies, real estate sector).

Faced with the need to accompany their clients' digital transformation and incidentally to generate business, corporations have been the first to develop their own set of metrics. The most well-known corporate indicator of building smartness might be the Honeywell Smart Building Score (HSBS) compiled by Fortune 100 American conglomerate Honeywell (NYSE-HON). The HSBS is a universal framework that can be used as a self-assessing scoring tool by the company's existing and potential clients globally.

The HSBS covers three characteristics: greenness (environmental sustainability); safety (security of the building, its occupants, users and owners); and productivity (through comfort and productivity enhancement for users and owners). These characteristics are captured by 'active components' (such as devices, software and analytics) on which Honeywell explains it can add

THE HSBS COVERS THREE CHARACTERISTICS: GREENNESS (ENVIRONMENTAL SUSTAINABILITY); SAFETY (SECURITY OF THE BUILDING, ITS OCCUPANTS, USERS AND OWNERS); AND PRODUCTIVITY (THROUGH COMFORT AND PRODUCTIVITY ENHANCEMENT FOR USERS AND OWNERS).

value. So-called "'passive components' - that is, architectural design, building location and building materials - are overlooked.

Hence, the HSBS seems to be best suited for property owners looking to smart up their properties by using Honeywell's solutions rather than those aiming for a holistic view of what a building should include in order to qualify as smart. Noticeably, scoring methodologies defined by corporations tend to be biased towards their sponsors' product and service offerings.

Public Versus Private Indices Of Smart Buildings

The alternatives to corporate indices of smart buildings are public indices developed by industry organisations, academics and/or governments. These indices are usually closer to certifications than scores. As many countries have adopted different key performance indicators (KPIs) for smart buildings, public indicators of smart buildings embody deeply rooted and diverging interpretations of smart buildings' essence and contributions to smart urban environments across the globe.

While Europe's Smart Readiness Index (SRI) promoted by the European Commission Directorate-General for Energy is geared towards sustainability, the US (with the Building Intelligence Quotient or BiQ) emphasises the performance and cost effectiveness of smart buildings.

By the same token, Asian countries have adopted a wide range of indicators with very different KPIs. In South Korea, one of the global leaders in smart technologies, intelligent building indices focus on smart features only, as sustainability is assessed by a separate certification initiated beforehand by the government. In Japan, the focus is on services derived from smart features whereas China emphasises system aspects.

Interestingly, Asia has been at the forefront of smart building index development. The first index of building intelligence ever published - the Intelligent Building index (IBI) - was introduced by the Asian Institute of Intelligent Buildings in Hong Kong in 2005.

Irrespective of their KPIs, most existing scores encapsulate an engineering view of smart buildings. Such a view defines smart buildings as highly sophisticated, self-contained 'machines', by emphasising their technology rather than their interactive dimension.

Despite covering a wide array of elements, these public indices overwhelmingly ignore a building's ability to interact with its smart urban environment, which is a source of both efficiencies instrumental to a smart city's success (for example, buildings as prosumers in smart energy grids) and risks (for example, data breach on connected ICT networks).

Hence, in their current versions, both private and public indicators of smart buildings fail to capture the complex and growing role that buildings will play in smart cities - as data collectors and connected platforms that turn buildings into 'ibuildings'.

The Importance Of Cyber Risks In Assessing Smart Buildings

One important dimension of smartness for all stakeholders should be cyber risks posed by technologies embedded in smart buildings. The issue of cyber risk concerns not only buildings' occupants (with potentially catastrophic scenarios worthy of horror movies), but also corporations operating in this kind of space.

One should not forget that real estate has been targeted in numerous breaches of cybersecurity in recent years. In a note entitled Cybersecurity - Securing Real Estate Assets In A Digital Age (January 2019), ANREV reminds us that in 2013, hackers gained access to up to 40 million debit and credit card records of American retail giant Target's shoppers through information stolen from the company's heat, ventilation and air-conditioning operator. In 2017, Target reported that the total financial cost of the hack amounted to US$202 million.

INTERESTINGLY, ASIA HAS BEEN AT THE FOREFRONT OF SMART BUILDING INDEX DEVELOPMENT. THE FIRST INDEX OF BUILDING INTELLIGENCE EVER PUBLISHED - THE INTELLIGENT BUILDING INDEX (IBI) - WAS INTRODUCED BY THE ASIAN INSTITUTE OF INTELLIGENT BUILDINGS IN HONG KONG IN 2005.

As IoTs, sensors and ever more potent cyber physical systems multiply in the very fabrics of our future cities and buildings, the scope and intensity of cyber risks stemming from smart building technologies can be expected to increase exponentially in the future. Such threats should be clearly identified, assessed and known to potential users and owners of smart buildings. Fire and security systems are clearly not enough anymore.

To achieve that, all stakeholders should be involved in defining the criteria that make a building smart, not just vendors with a vested commercial interest. Sound smart building certifications will be an important component of a functioning market for smart real estate. This is a necessary step towards promoting investments in this new segment of the commercial property market and, more fundamentally, fostering public confidence in smart cities. SST

This commentary first appeared in The Business Times.

Cloud-Native Solutions Are Revolutionising Smart Buildings

▸▸ By Harbor Research

Today, all electronic devices are becoming connected in an ever more distributed and pervasive way, enabling the convergence of physical and virtual worlds.

These networks of intelligent, connected machines are the world of smart systems, a new generation of information architecture that — when combined with cloud computing, artificial intelligence, machine learning and Internet of Things (IoT) technologies — represents a radical break from yesterday's information, computing and telecom (ICT) paradigms.

Core Technologies Are Enabling Opportunities In Smart Building Systems

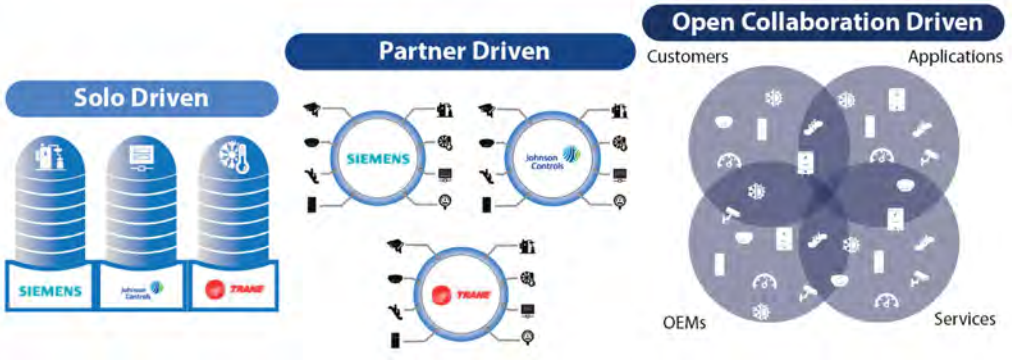
Smart systems in the buildings sector are entering a dynamic period with emerging solutions across all segments that will result in OEMs, technology suppliers, third-party value-adders and users needing to leverage, react to and monetise emerging technologies in different ways.

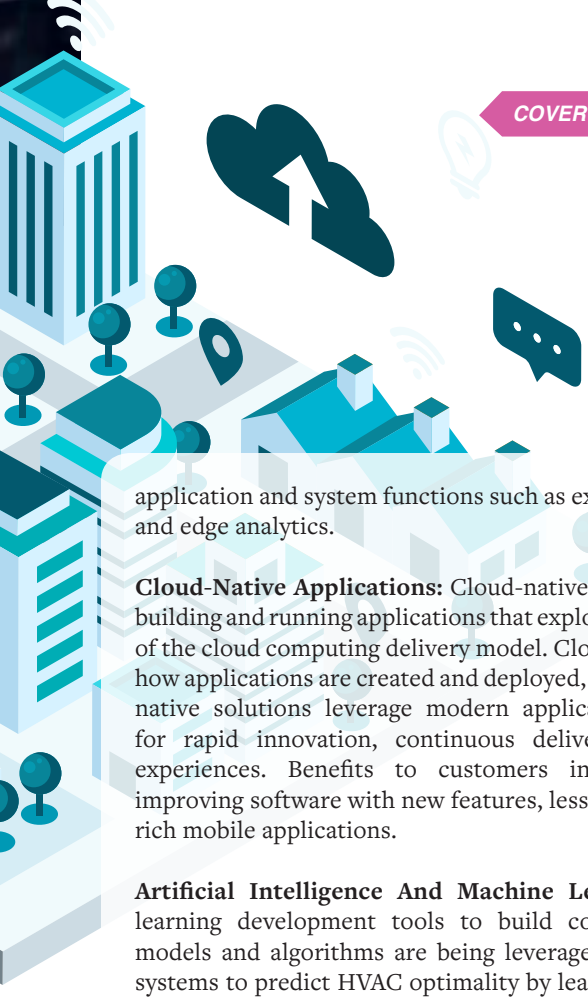
The key technologies that are driving change in buildings include:

Sensors, Actuators And Machine Data Fusion: The cost of devices, and the marginal cost of storing the data generated from them, will continue to plummet with advances in silicon, packaging and integration technology. Component miniaturisation and the integration of a broad range of sensing capabilities into intelligent devices will continue to provide a variety of features that support the integration of digital information and sensory inputs.

High-Performance Networks And Infrastructure: The current fragmented landscape of proprietary device networks is beginning to give way to a new generation of wireless communications developed for challenging environments such as buildings.

Distributed Data Management: Systems designed for distributed capture, computing and control are enabling new





application and system functions such as exception reporting and edge analytics.

Cloud-Native Applications: Cloud-native is an approach to building and running applications that exploits the advantages of the cloud computing delivery model. Cloud-native is about how applications are created and deployed, not where. Cloud-native solutions leverage modern application frameworks for rapid innovation, continuous delivery and superior experiences. Benefits to customers include constantly improving software with new features, less IT headaches and rich mobile applications.

Artificial Intelligence And Machine Learning: Machine learning development tools to build complex predictive models and algorithms are being leveraged within building systems to predict HVAC optimality by learning from droves of past data. Algorithms can even take into account factors outside of buildings such as weather, pedestrians, traffic and more. These new capabilities turn data into contextualised awareness and knowledge.

User Experience (UX/UI, AR, VR) And Services Interaction: As more devices in buildings become connected and start emitting sensor data, new user experience (UX) tools are being created to drive services delivery. An example is modern logic programming that allows building operators to create simple interactions between devices with more complex underlying algorithms executing the logic.

Semantic Data Tagging: Standardised methods for describing data are being brought to market, making it easier to analyse, visualise and unlock additional value from the vast quantity of data being generated by devices from a range of vendors within buildings.

Self-Tuning Controls: Integration of wide-ranging sensor data is enabling collective awareness of building state, which dynamic control systems are leveraging to adjust building parameters including set temperature, heating/cooling schedules and light lumens. Control systems react to inputs, including exterior temperature, weather forecasts, ambient light, occupancy and learned user preferences to optimise the environment based on real time, user-specific cues.

Suppliers are Evolving, but Few Serve Customer Needs Well

In the present buildings landscape, significantly different business processes are required to take advantage of smart systems. Even many of the players that are primed to capitalise on the new opportunities of smart systems in buildings are unsure how to change their business model in accordance with these new technologies.

Equipment suppliers, contractors and engineering firms are purely transactional and walk away following the completion of a project. Evolving customer expectations are forcing suppliers to prioritise user-centric design with end-to-end systems and services, challenging not only technical solution design but also legacy business models and channel structures.

As building providers move toward smart systems, many are trying to do so by simply adding capabilities without considering the need for an intricate and interoperable ecosystem, resulting in significant end users challenges. Without open and flexible data and application tools, building operators are left with several different systems to navigate before getting a holistic picture of their building systems.

Conclusions

The buildings space presents a perfect environment for smart systems to radically re-order traditional industry limitations and move to a continuous improvement model for smart building solutions.

Emerging cloud-native providers are leading the charge to capture innumerable data points and turn them, within milliseconds, into predictive, actionable opportunities. Thanks to the combined processing power of edge and cloud computing, this potential has arrived today. Advances in big data analytics and AI are positioned to make self-adaptive buildings a reality via continuous feedback loops between building equipment and software.

Although new technologies surrounding the intelligent buildings space have unlocked the ability to generate more value for OEMs, service providers, and end users alike, there are several intractable non-technological challenges. A lack of understanding of the immense value provided by native cloud, as well as resistance from OEMs and service providers to move from on-premise solutions, has inhibited the growth of smart systems in buildings.

Traditional technology suppliers such as building automation OEMs are trying to leverage old solutions to address new demands, keeping archaic data architectures that prevent them, and their service providers, from creating ongoing digital services around their products. The longer they delay in defining data as an asset, and seeing the cloud as the delivery vehicle for ongoing customer relationships, the farther they will drift from a smart systems strategy. SST

This is an extract from Harbor Research's whitepaper titled Revolutionising Building Management With Cloud-Native Solutions

How Video Analytics And Warehouse Management Software Unite To Secure This Brazilian Warehouse

Warehouses are complex security environments. Hundreds of workers move thousands of items through aisles and corridors, making it difficult for Security Managers to detect inventory theft and track missing shipments. In an Industry 4.0 success story, the team at the Bosch Automotive Aftermarket distribution centre in Itupeva, Brazil, used the Internet of Things (IoT) to create a solution: Their customised integration between video analytics and warehouse management software prevents theft, heightens efficiency and improves shipment tracking.

Located about 70 kilometres from São Paulo, the automotive distribution centre in Itupeva is a central hub for the entire South Americas region. The 26,000-square-metre facility processes 68,000 shipments of key components per year, so the sheer level of movement of items, pallets and warehouse personnel proves challenging to track from a logistics and security perspective. A few years ago, the logistics team realised that inventory losses from theft were on the rise. Meanwhile, customer inquiries about misplaced items in shipments required lengthy research, putting the centre's reputation at risk. This called for a change of approach.

Investigating the issue, it turned out that the security team was overwhelmed by the sheer amount of alarms. Every incident recorded by the video cameras required time-consuming manual investigation. Whenever an employee entered a restricted aisle, personnel in the security control room received an alert to perform a cross-check in the warehouse management system. This was to confirm whether an active task had been assigned to that aisle. If not, security on the warehouse floor would be called to investigate. But with thousands of alerts and false alarms per day, this proved humanly impossible.

To solve the challenges, the Bosch experts worked for over one year to automate the time-consuming manual checks. The approach combines the Intelligent Video Analytics technology built into Bosch cameras with a customised configuration of the Bosch Video Management System and an interface to the centre's warehouse management system.

From a technical perspective, it's an ingenious combination of existing technology with networked information: All of the distribution centre's 200 security cameras, including the high-definition Bosch

> "Because every check in the warehouse system was conducted manually, it led to a situation where security operators could not verify the large number of security events."
>
> ***- Mario Verhaeg, Product Manager at Bosch Building Technologies***

"This is a real Industry 4.0 success story. The solution is technically complex and involves a high level of customisation. But it's a nice showcase for what is possible to achieve within these systems when the right resources and creative people get involved."

- Mario Verhaeg, Product Manager at Bosch Building Technologies

Flexidome IP series, are fitted with Intelligent Video Analytics. This built-in function processes image data in real time and detects suspicious activities by means of an algorithm. In the first step, the team 'taught' the cameras to recognise objects in the warehouse such as forklifts and shipment items. Once the security system had learned to identify these objects, it was ready to interface with the centre's logistics system.

In the next step, the team created a direct interface between the warehouse management system and the Bosch Video Management System. Creating the connection adds a new level of intelligence to the centre's video surveillance: The smart cameras now act as IoT sensors that can identify products stored in the warehouse management system software, which currently catalogues 13,497 part numbers. The system also automatically cross-checks security incidents with scheduled tasks in the warehouse system. Thanks to this smart automation, operators only receive alarms when a worker enters an aisle without a task – and no alarm is triggered if the worker passes through without stopping. As a direct result, the number of security events dropped from several thousand to about 100 per day and incidences of theft receded as well.

From an operations perspective, the Industry 4.0 solution not only boosts security but also answers the centre's need to replace the time-consuming manual tracking process for misplaced items and shipments. Whereas the logistics team previously required several hours to manually locate a lost item, every item now receives a tracking number connected to video recordings documenting its movements. This level of transparency allows the logistics team to solve inventory problems within minutes instead of hours.

Ever since the system has been successfully rolled out, the team in Itupeva has used the new level of oversight to unlock additional benefits: Four solid fences guarding sensitive areas in the warehouse could be replaced by 'virtual fences', meaning security zones defined in the video management system. This unlocks a new level of flexibility for changing the arrangement of aisles and shelves in the warehouse – as is frequently required – entirely without compromises on security. What's more, the customised Industry 4.0 solution drastically reduces inventory costs by performing 'virtual inventory' in real time and is expected to amortise itself in less than a year. SST

Biometric Applications: Have They Reached A Security Tipping Point?

►► **By Matan Scharf,**
Senior Security Solutions Manager at Synopsys

This is the biometric age with biometric methods of identification soaring in popularity.

Today, almost every modern smart mobile device features fingerprint scanners and voice and facial recognition as the default mechanisms for access control.

As their adoption grows, their application is also expanding in scope to enable features such as app purchase and in-app payment, e-wallets and access to password managers.

From an IT systems administration's perspective, the advantage of these methods of identification over passwords, even one-time passwords (OTP) and two-factor authentication (2FA), is the great difficulty of faking a biometric sample or manipulating the biometric sensor into producing a false-positive result.

For many years, this last statement stood largely unchallenged. However, at this moment, amidst the proliferation of biometric applications in the consumer market (and specifically mobile devices and IoT), we are possibly looking at the tipping point for the security of biometric applications.

This tipping point centres around two major concerns surrounding biometric identification methods:

#1. Are biometric methods of identification as secure as we assume they are?

#2. What new risks do we face in the short and long term with regard to privacy and the risk of irreversible identity theft?

The Maker/Hacker Paradigm In Biometric Applications

The recent news about the Samsung Galaxy 10S+ fingerprint hack is extremely interesting to contemplate in relation to this tipping point.

In this social media event, a researcher 3D-printed a resin mold of his own fingerprint. He then demonstrated via image sharing website Imgur how that resin mold could be used to unlock his own Samsung Galaxy 10S+ device.

We need to treat this finding with a certain level of caution. In the video demo it appears as if he was unlocking the device with the resin mold while wearing a glove—and yet he is holding it with his index finger. One might assume that this is the same finger used to unlock the device.

The initial impression is that the researcher was able to crack an industry-grade fingerprint reader using commoditised technologies (cell phone camera, commercially available 3D printer and software).

To assess if that is indeed true, it is important to understand how the Qualcomm Snapdragon Sense ID Fingerprint Sensor (which is used by the Samsung Galaxy 10S+ device, among other devices) works.

Not All Biometric Methods Are Created Alike

Ascertaining a user's identity using a fingerprint involves several steps. One must collect the sample, remove the noise (such as dirt and blur from miniscule movement), extract the key features and calculate the match to the baseline sample. There are also controls around the detection process to ensure that the reader is scanning a real, living human finger. Despite the common misconception that fingerprints are matched by checking the overlap or visual similarity of two images, modern algorithms do not actually work this way. Algorithms are based on mathematical models that identify families of features (such as ridges, lines and gaps) and build a mathematical expression of these features; for example, the distance between the centre of one shape pattern and a distinctive line. This probabilistic approach allows for a much faster and more accurate calculation, while also avoiding the need to retain an image of the original sample on the device, thus preserving the user's privacy.

When it comes to fingerprint readers, there are a few basic methods for performing the first step of collecting the sample. The methods include: optical, capacitive, ultrasound, e-field, electro optical, pressure sensitive, thermal and MEMS (microelectromechanical systems).

Of these, three are commonly used in modern smart phones: capacitive, optic and ultrasonic.

In the capacitive method, the fingerprint surface is scanned onto a 2D grid of a conductive sensor that detects the minute electric capacity differences caused by the skin folds that make up the ridges and valleys of a fingerprint.

In the optic method, a 2D image of the creases and folds of the surface is collected by detecting the absorption, scattering and reemitting of a source of illumination (such as LED or laser).

In the ultrasonic method, a 3D image of the fingerprint is sampled by measuring the variant of the echo produced by the skin folds of a fingerprint.

The fingerprint sensor that Samsung uses relies on the last method. According to Qualcomm, this method has an advantage over other methods as it can scan deeper and produce more accurate results in creating a 3D image compared to the 2D image rendered in other methods. Additionally, it features a built-in liveness detection algorithm.

According to official documentation, the scanning supports material penetration technology that allows the sensor to scan through glass, plastic, aluminum and more. It could be this depth that is the culprit in this case — the researcher may have used the same index finder to press down the resin mold. Naturally, this would also defeat the liveness detection mechanism.

"When it comes to fingerprint readers, there are a few basic methods for performing the first step of collecting the sample. The methods include: optical, capacitive, ultrasound, e-field, electro optical, pressure sensitive, thermal and MEMS (microelectromechanical systems)."

> ***There are alternatives to the more traditional biometric solutions (for example fingerprints, retina and voice recognition) such as cognitive and behaviouristic methods that could offer a good balance between level of security and the revocation/natural decay of the baseline as people's cognitive abilities and behaviours gradually change over time.***

Should We Run For Cover?

This maker/hacker approach to circumventing biometric identification is nothing new. A hacker by the name Jan Krissler demonstrated over four years ago how he could fake the fingerprints of the German defense minister, Ursula von der Leyen, using a photograph released by her own PR office. Knowing this, should we be concerned? The simple fact that it is feasible doesn't necessarily make it probable. For this risk to become a significant concern, the attack surface must change and evolve into a scalable vector that can be automated, at least to a certain degree. In other words, as long as the biometric application is paired with a specific physical device that the attacker must have physical access to, the likelihood of this threat affecting the general public is relatively low. We can still expect to see weaknesses published by researchers whose main motivation is pulling off a technical conquest and attaining recognition as opposed to the cybercriminal and hacker counterparts who are driven by profit and the quest to monetise the weaknesses they uncover.

Regardless of the validity of this specific experiment, this episode is an excellent example of the inherent tradeoff between the convenience of not having to type passwords and the risk of having an authentication/authorisation mechanism lacking a revocation mechanism.

The Future Of Biometric Identification

We can expect biometric identification to continue to grow in popularity and expand in application scope. Hot trends, including IoT applications for smart homes, e-voting and biometric border controls, will intensify interest among the hacking community to make attempts.

To overcome these risks, we need to consider adding additional layers of anti-fraud or business intelligence where applicable (that is, identify suspicious/abnormal application activity, use GPS to correlate identification events and so on) to the applications using biometric identification to reduce the risk of misuse or fraud. In this way, we can make it as difficult as possible for malicious agents to complete fraudulent transactions.

We have yet to reach the tipping point in which the potential weaknesses in biometric applications of identification/authentication are a major concern. I would argue that compared to passwords, biometric identification is still a much more secure method, despite its inherent flaw of lacking the revocation mechanism.

However, while we are not at the tipping point yet, we should be sensitive when applying biometric solutions that might drive us to that tipping point.

There are alternatives to the more traditional biometric solutions (for example fingerprints, retina and voice recognition) such as cognitive and behaviouristic methods that could offer a good balance between level of security and the revocation/natural decay of the baseline as people's cognitive abilities and behaviours gradually change over time. SST

INSIDE LOOK

Cloud Security Is Changing The Security Channel Partner Model

►► **By Scott Robertson,**
Vice President of Asia Pacific and Japan, Zscaler

Digital transformation and cloud security have led to a dramatic shift in how enterprises manage their applications and infrastructure. These two trends have developed into business necessities and have also changed the relationship between enterprises and their channel partners.

In business, there's always a bit of tension between a buyer and a seller. By definition, in an exchange, both sides need to feel as if they're getting a good deal. In just about any deal, there is an agreement on a price but a difference of opinion on the actual value. For instance, when you sell your house, you're happy to sell it for a certain price and somebody else is happy to buy it, but each side has different motivations.

That dynamic tension is even more pronounced in the world of technology. With the large, complicated technology deals that companies and vendors construct, many enterprises create a partner network designed to take care of the needs of the business. But naturally, the partner network also has to take care of itself. This can lead to a delicate balance that can be all too easily disrupted when it becomes clear that the partner is taking more care of itself than of its client.

Right now, these types of disruptions are happening frequently in the cybersecurity market as companies shift toward cloud-based cybersecurity services. The partner ecosystem that currently exists is dedicated to, and designed for, the world of the past where different software or hardware appliances needed to be integrated

and managed. Many vendor partners are resisting any change to this world because their very existence is predicated on being able to make money managing and selling actual devices and supporting integrations between them. In this new world, however, there isn't the same need for these services or products because much of cloud security has moved away from appliances.

Don't get me wrong: companies still need partners, especially when it comes to enterprise technology as large corporate networks are so complicated to configure and optimise. Businesses still need outside experts. But partners need to evolve what they bring to the table and how they approach their offerings.

We're already seeing this evolution as new partners and vendors born in and designed specifically for the cloud are motivated to manage and integrate cloud services that don't involve selling physical hardware or babysitting infrastructure over the course of its lifetime. Managed service providers in the cloud are focusing more on adapting to a company's processes and making their services fit individual businesses.

The consequence of this evolution of partner-enterprise relationship is that many companies are trying to figure out who their best partners will be for the future while juggling a complete digital transformation. Companies still need stability in their security, even in the cloud-based world, but their partners of old might not be able to provide this.

Some traditional partners are already recognising this new playing field. They have begun redesigning their business and incorporating small, born-in-the-cloud consultancies and security practices as part of their service offerings. But partners must fully accept that the past is the past – the world of selling a hardware box and then making money ad infinitum from managing it is gone.

That's why companies find purpose-built platforms, such as Zscaler's, so appealing. We manage the complexity of the cloud-based environment so that companies can achieve significant cost savings and efficiencies by replacing their hardware and system integration with a cloud-based focus – and achieve all this with industry-leading cloud security.

Companies are responding to these born-in-the-cloud partners because of the specialisation of their offerings and because they are much nimbler than partners still dedicated to selling servers. That's why I expect to see more niche cloud-based partners spring up and uproot many of the established technology partners that are clinging to the past. SST

> ***"Digital transformation and cloud security have led to a dramatic shift in how enterprises manage their applications and infrastructure. These two trends have developed into business necessities and have also changed the relationship between enterprises and their channel partners."***

Tips For World Password Day by Synopsys

►► **By Nabil Hannan,**
Managing Principal (Financial Services, Software Integrity Group), Synopsys

With many password leaks on the internet, organisations are starting to realise how important it is to store passwords securely in their applications.

Storing passwords securely is not quite as straightforward as just hashing or encrypting the password and storing it.

The trends I'm currently seeing in the industry are:

1. Organisations are moving away from just username and password model (1 factor) to a 2 factor authentication model to protect their users in the event that their passwords get breached

2. Social logins are gaining popularity and becoming easier to integrate. Organisations are leveraging social logins to make signing up/authentication easier for the end user.

Top Password Best Practices

For organisations, it is crucial to institute the practices of having strong passwords, regularly having users change their passwords and making sure passwords are stored securely.

> ***Social logins are gaining popularity and becoming easier to integrate. Organisations are leveraging social logins to make signing up/authentication easier for the end user.***

For end users, smartphones, tablets and personal computers have software available that manages and synchronises your passwords across devices (such as Apple's iCloud Keychain and Google Chrome's password manager). There are also other paid passwords managers that end users can use. End users can use their chosen password manager to generate strong and unique passwords and manage the passwords across the end user's different user accounts and machines.

Are Passwords Passé? If So, What's The Future?

Although using passwords may not be the most secure way of authenticating, it's simple and people have gotten used to using passwords. It is the most familiar and common form of authentication.

Eventually, passwords will become obsolete, and new authentication techniques leveraging social logins, single sign-on and biometrics will start to gain more traction. Ultimately which solution is adopted in the future will depend on which solution the end users end up using the most.

In A Nutshell

Passwords are just like any other sensitive data/asset of the software ecosystem. In order to design a system securely, organisations have to do the necessary business analysis to understand the importance of the data, do threat modelling to understand what controls need to exist to protect the data from threat actors, and then ensure those controls get included in the software requirements so that they actually get implemented and tested as part of the Secure SDLC. SST

10 Steps To Strategic Data Management

►► **By Scott Baker,** Senior Director of Emerging Business and Data Intelligence at Hitachi Vantara

There's no question that today's smart, connected business environment demands intelligent data governance. But the prospect of defining and implementing a data governance programme may seem daunting to many companies.

The typical business is overwhelmed with information about internal operations, customers, trading partners, competitors, employees, finances and other strategic concerns. And it has to meet many demands. Regulators and compliance officers require certain information to meet extremely specific standards. Security experts demand that sensitive data be adequately protected.

Furthermore successfully executing top-level strategy depends on gathering all relevant data, analysing it, and applying the resulting insights to the company's most pressing challenges.

The typical business may find this list of requirements off-putting and may wonder where and how to get started on achieving strategic data management.

Here are 10 keys to successfully establish an intelligent data governance programme that will deliver significant, continuing value across the enterprise.

1. Ensure data is complete and accurate. Data consistency is one of the biggest benefits of enacting a data governance initiative. Only high-quality data can form the basis for sound business decisions and drive the company in the right direction.

2. Conduct proactive data quality checks.

3. Align data to regulatory and compliance guidelines.

4. Eliminate data confusion.

5. Connect data and analytics to top-level goals. Intelligent data governance means making sure the right data is moving through the information supply chain in the right flow and with the

right structure, to achieve the company's highest-level strategic goals.

6. Encourage fact-based, real-time decision making. Change occurs constantly and companies need to react swiftly. Having the right data available, in the right format, drives real-time decision making and generates a high-level of confidence.

7. Create a data-centric culture. Gathering, analysing and applying data isn't the job of one department. By encouraging everyone to share insights and by centralising data access, companies can make better-informed decisions at every level.

8. Foster collaboration and establish accountability.

9. Store information more effectively. Virtually every company is either storing data that is irrelevant or storing relevant data for too long. Developing standardised rules and policies ensures that data storage is conducted strategically and cost efficiently — and makes everyone a steward of the shared information.

10. Harness data as a competitive advantage.

> ***"Encourage fact-based, real-time decision making. Change occurs constantly and companies need to react swiftly. Having the right data available, in the right format, drives real-time decision making and generates a high level of confidence."***

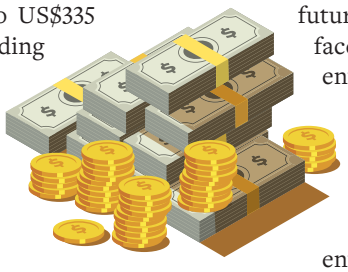
If this list seems intimidating, it's important to remember that companies don't have to do it alone. There are powerful, automated solutions available today that can streamline and accelerate even the most complex data governance tasks. There's no need for any business to re-invent the wheel when technology leaders have already developed customised solutions targeted directly at addressing the challenge of intelligent data governance.

With these advanced solutions easily available, the only real question for executives is: why isn't your company doing a better job of governing data more intelligently? SST

Threats Will Drive Cities' Resilience Spending To US$335 Billion In 2024

City governments worldwide are becoming increasingly aware of the importance of enhancing their cities' ability to withstand or recover quickly from a range of predictable and unpredictable disasters and catastrophes.

This will drive global public spending on urban resilience projects from US$97 billion in 2019 to US$335 billion in 2024, according to a new report from ABI Research, a market foresight firm offering insights into transformative technologies.



"Due to their very high population concentrations, cities are much more vulnerable to the catastrophic potential of earthquakes, tsunamis, volcano eruptions, sea level rise and flooding, food shortages, wildfires, extreme heat, hurricanes, tropical storms and typhoons, terrorist attacks, civil unrest, cyber attacks, war, diseases and epidemics, nuclear or chemical contamination, extreme air pollution and many other emergency situations. So much so that many cities have already appointed a Chief Resilience Officer," explained Dominique Bonte, Vice President, End Markets at ABI Research.

While the smart cities concept is very much geared toward ensuring liveability of citizens in the present, resilient cities guarantee future liveability in the face of a changing urban environment not only in terms of acute shocks but also in terms of chronic stresses related to economic, financial, environmental, social and institutional crises.

Growth in global public spending on urban resilience projects will be from spending on both physical infrastructure and ICT infrastructure and services.

Resilience spending is currently led by cities in developed regions. The cities of New York and Miami Beach have announced budgets of US$500 million

and US$400 million respectively for flood prevention, mitigation of sea level rise and coastal areas reinforcement. By 2024, cities in developing regions will account for 40% of all resilience spending, said the report.

Resilience strategies and solutions include many components ranging from detection and prediction via advanced sensors and AI-based analytics to alert systems, evacuation procedures, rescue missions and relief response modes in the immediate aftermath and recovery for survivors and the city as a whole in the longer term.

“Resilience strategies and solutions include many components ranging from detection and prediction via advanced sensors and AI-based analytics to alert systems, evacuation procedures, rescue missions and relief response modes in the immediate aftermath and recovery for survivors and the city as a whole in the longer term.”

Critical resilience technologies and paradigms include predictive modelling and digital twins (already explored by cities like Cambridge, England and Rotterdam, Netherlands), cybersecurity, redundant infrastructure and system designs, decentralised service provisioning, demand-response optimisation, sharing economy and cross-vertical integration, physical robustness and robotics.

Key suppliers of resilience technologies covered in the report include NEC, Bosch and ZTE. Organisations like 100 Resilient Cities (100RC), the United Nations (Making My City Resilient campaign), and the U.S. National League of Cities (Leadership in Community Resilience programme) are promoting best practices for designing resilient cities.

“Resilience programmes for dense urban areas are closely linked to sustainability efforts aimed at preventing pollution and mitigating the impact of climate change on flooding and other severe weather conditions. According to Lloyd’s City Risk Index, climate-related risks alone account for US$122.98 billion of Gross Domestic Product (GDP) under threat for a sample of 279 cities. With cities being centres of economic activity, minimising loss of GDP is the most important incentive and justification for resilience spending in terms of Return on Investment,” Bonte concluded.

These findings are from ABI Research’s Resilience Technologies and Approaches for Smart Cities application analysis report. This report is part of the company’s Smart Cities and Smart Spaces research service, which includes research, data and executive foresights. SST

Securing The Smart Ecosystem

►► **By Amit Mehta,**
Managing Director,
BlackBerry ASEAN

Singapore is among the world's most stable economies, averaging a growth rate of 3% to 3.5% in recent years. Churning out a GDP of approximately $487,088 million in 2018, the city-state continues to strive for improvements in productivity, income and quality of life. To continue supporting the country's growth through rapid urbanisation and increasing urban density, it is also crucial for Singapore to explore solutions that help the country to become secure, smart and sustainable.

The Smart Nation movement was launched by the government in 2014 as a national effort to tackle critical needs such as transport, housing and medical care through the integration of technology. By embracing and facilitating such seamless solutions, Smart Nation aims to benefit Singaporeans, government agencies and businesses by revolutionising the way its people and organisations live, work and grow.

It is already setting global standards. The Smart City Expo World Congress in Barcelona named Singapore the 'Smart City of 2018'. Present at this congress, Dr Janil Puthucheary, Senior Minister of State and Minister-in-charge of GovTech said, "Singapore's Smart Nation efforts are about the transformation of our country through technology. We will continue to create a better lived experience for our citizens, and these efforts must benefit our future generations as well."

The Upside And Downside Of A Connected Society

As mobility and technologies like Artificial Intelligence (AI) and Machine Learning (ML) continue to change how we live and work, people and things will become far more susceptible to a wide range of threats and increased risks. This reliance on technology threatens individuals, businesses and governments as threat surfaces increase and expose data and information. This is especially true as the infinite supply of data becomes more interconnected in infrastructure and daily operations, whether that is data shared between people, between machines or all the above.

One of the most urgent matters that the country must tackle in its Smart Nation initiative is to secure data protection, privacy and safety of all businesses and its residents. Recent episodes of data compromises and cyber attacks in public sector agencies like SingHealth and financial institutions like AXA insurance underline the urgent need for safeguard measures, skills development and security by design. Like any smart ecosystem, we must first ensure that government and private organisations provide trusted systems, training and business continuity procedures to combat potential cyber-related crises head-on.

Data Protection And Trust: The Key To A Smart Ecosystem

In this digital age, data is one of society's most fundamental assets. Big data has the power to convey insights and assist in decision making and actions required to solve everyday problems. At the forefront, data can be used to develop something as simple as cashless payments. Take for instance, PayNow, a banking service in Singapore that allows one to send or receive money in an instant using the recipient's National Registration Identity Card (NRIC) or mobile number.

But it is a fine balance, particularly for government and other industries like finance, health and online services that are facing a technology trust crisis. Millions of businesses and people trust institutions with personal and business critical data. How can they be assured that their data is both secure and private?

With connectivity comes responsibility. At BlackBerry, we believe it is the economic, social and ethical responsibility of technology leaders to build security and privacy into their products by design. This request is not a tall one.

> ***"Singapore's Smart Nation efforts are about the transformation of our country through technology. We will continue to create a better lived experience for our citizens, and these efforts must benefit our future generations as well."***

First, build products that have security ingrained in each layer and commit to ensuring the product has no backdoors. Second, respect that an individual's personal data is his and do not profit from the data or use it without his consent, which must be transparently obtained.

BlackBerry is in the business of protecting data – not monetising it – and is focused on helping industries around the world to keep data and people safe, so they can get on with business. One example of this is the delivery of complete endpoint management and policy control for a wide range of devices, connected end-points and apps with BlackBerry's Unified End-Point Management (UEM) software. One of the largest banks in Indonesia, Bank BRI, uses BlackBerry's UEM software in their back-end management. By empowering the bank to protect the financial data of its customers and allowing employees to collaborate more effectively, Bank BRI can be proactive in mitigating cyber risks.

Tightening Security Measures

For Singapore to progress towards its Smart Nation goals, information must be secured at every layer (devices, software, apps and networks) to minimise potential threats.

For instance, there are 'smart lamp posts' in Singapore equipped with a network of wireless sensors that observe unusual/illegal street activity and climate change through functions like facial recognition, noise detection and

environmental sensors. By taking a holistic approach to safeguarding our nation with secure software, we can mitigate cybersecurity-related risks, data privacy and help prevent manmade disasters.

Equipped with deep understanding and knowledge about the rising demand for trusted connectivity in rapidly growing smart cities, BlackBerry has developed several tools that incorporate advanced security measures.

The BlackBerry Security Credential Management System (SCMS) provides a trustworthy and private space in which information exchange can take place for vehicles and infrastructure. Through the optimisation of BlackBerry's Certicom technology, devices like traffic lights, for example, can tally received information using digital certificates.

BlackBerry also offers a networked emergency or crisis communication platform that helps any industry with a duty of care to keep people and assets safe, such as government and defence, industrial and manufacturing, private enterprise, healthcare and transportation. It protects over 70% of the US Federal Government agencies, including the US Airforce and Department of Defence and is also used by education institutions such as Macquarie University in Australia to keep staff and students safe. In Canada, Durham Regional Police Services uses it for automating critical alerts, enabling it to more quickly reach out to first responder personnel beyond text messages and email.

Hyperconnectivity Leading The Path To Transforming Our Lives

Gartner predicts that 14.2 billion connected things will be in use by 2019, and this number is expected to reach 25 billion by 2021, producing an immense volume of data. Putting this into perspective, hyperconnectivity is set to become the next step in revolutionising the way people work and live.

In Singapore, more and more smart technologies are being developed to assist the rising needs of society. For instance, there are medical and life support systems in local hospitals that can be activated for elderly patients requiring immediate critical care.

In such a hyperconnected world, cybersecurity is not just about protecting data, but also protecting people – the secure flow of information is both mission- and safety-critical. Because when everything is connected, everything is potentially a target. Should even a single endpoint in a system be unprotected, nothing is secure. BlackBerry's term for this is the Enterprise of Things (EoT), and its mission is to provide support for all organisations to securely manage and control all physical and digital endpoints.

> ***By having the right systems in place that offer solutions like end-to-end encryption, threat detection and prevention, IP/file protection and collaboration, this technology will enable secure connection with the smart ecosystem and advance an organisation's own digital transformation strategies.***

By having the right systems in place that offer solutions like end-to-end encryption, threat detection and prevention, IP/file protection and collaboration, this technology will enable secure connection with the smart ecosystem and advance an organisation's own digital transformation strategies.

The unimaginable is becoming a reality. Medical devices and embedded sensors are now connected to virtual assistants. Technology-backed secure solutions and services provide endless opportunities within realms like crisis communications. And collaborative, unified endpoint management is now enabling the security of smart cities.

Moving Forward

Fundamentally, interconnectivity is important as it lays the foundation for successful smart cities. However, harnessing hyperconnectivity to advance these projects means ensuring finely tuned management that secures data at every point and layer within the design of the ecosystem.

Investing in trusted, reliable software solutions that can keep data and people safe and secure will allow the Singapore government and industry to focus their efforts on driving efficiency, capitalising on opportunities and advancing Singapore's goals. It also essential to fight fire with fire with new technologies such as AI and ML that are fast enough to detect and prevent threats before they happen, protecting every single endpoint.

Bottom line, as a global leader in smart city innovation, Singapore must also strive to set global standards for a 'Smart Nation' that is as secure and safe as it is connected. SST

Public Cloud Platforms Are Not Waterproof

►► **By Nick Itta,** Vice President of Sales, APAC, EfficientIP

Digital transformations are occurring across Asia at a rapid pace, with more and more organisations, both public and private, transferring data onto the public cloud.

This trend is occurring in part due to the increasing recognition that cloud services are more convenient, less costly and more scalable than self-hosting and locally storing data within an organisation's own servers.

As more data is being moved to public cloud platforms like Google Compute Engine or Microsoft Azure, it is critically important that organisations do their due diligence and evaluate the security infrastructure of their public cloud provider. Organisations often assume public cloud platforms are wholly responsible for providing security in the cloud. However, recent product revamps by major public cloud services providers demonstrate that they are actually trying to remove some of that burden and placing the responsibility of securing aspects of the DNS in the hands of its customers.

Failing To Plan Is Planning To Fail

Many organisations do not even consider the possibility of their data being pilfered because they assume their public cloud provider is securing their DNS. This means that actual attacks go unnoticed.

Also, due to the high workload on most public cloud services, DNS security implementation is 'standard-built', thus allowing DNS tunneling, DNS file systems and data exfiltration

> ***To better guard against potential DNS attacks within the public cloud and secure sensitive business information, organisations should consider the deployment of a private DNS security solution in addition to the public cloud provider's existing security infrastructure.***

to occur. The reason most public cloud providers implement only 'standard' DNS security infrastructure is to allow ease of access and speed of access.

Failing to adequately secure the DNS on public cloud platforms has potentially serious ramifications. A rudimentary DNS security infrastructure allows for a wide range of possible data leaks. For example:

External: Malicious backend access of applications through the DNS performed via unsecured APIs, heap overflow and other methods can allow a hacker full visibility of a public cloud's data.

Internal: Persons inside the organisation who have access to a host can modify/install/develop an application that uses DNS to perform malicious operations against an organisation (such as push data or get malware content).

External: A malicious code inserted in a widely used library on the public cloud can potentially impact all users of the library.

Internal: Persons inside an organisation could insert a specific code that uses the DNS to extract data, events and other account information.

Even a temporary storing of sensitive business information on networks hosted in a public cloud can expose a business to aforementioned entry tactics. Visma, a Norwegian cloud-based service provider, was hacked by a hacker group backed by the Chinese government called APT10 using an external entry method. Fortunately, the hackers were only able to exfiltrate Visma's data and none of its clients' before the attack was detected.

To better guard against potential DNS attacks within the public cloud and secure sensitive business information, organisations should consider the deployment of a private DNS security solution in addition to the public cloud provider's existing security infrastructure.

Think of a private DNS security solution as the lock to a door of an apartment within a larger apartment building. While the apartment building has secure entry and exist methods, one would never think not to install door locks to one's own apartment. The same approach should be applied to hosting an organisation's sensitive data within the public cloud.

We do not advocate that public cloud providers restrict their DNS access. We understand public cloud providers need to be able to provide easy and timely access to their customer's data. However, we do believe private networks within the cloud should be deployed without DNS access. Instead, private networks should always be deployed with a private DNS security solution in place. SST

GLOBAL SMART BUILDING MARKET PROJECTED TO HIT US$61,900 MILLION BY 2024

Valued at US$5,800 million in the year 2016, the global smart building market is expected to be worth US$61,900 million by 2024.

The market will grow at a compound annual growth rate (CAGR) of more than 34% between 2017 and 2024 according to a report by Zion Market Research.

The ever-increasing consumption of energy and cost of energy is driving demand for smart buildings, describes the report. Smart buildings minimise the use of energy, optimise space and have less impact on the environment. Hence they allow facility managers and building owners to reap better asset performance. In particular, Zion's research analysts observed that there will be an increasing demand for energy management systems in the smart building market to allow building owners and managers to reap the benefit of efficient energy utilisation.

The market is made up of many subsectors, including commercial, residential, government, airports, hospitals, institutes and manufacturing and industrial facilities.

Also propelling the growth of smart buildings is the increasing demand for integrated security and safety systems and the ongoing push by governments for smart building programmes. And smart buildings are getting ever smarter. A growing number of smart buildings incorporate a slew of advanced technologies to manage lighting, energy, heating and security systems.

The market is made up of many subsectors, including commercial, residential, governmental, airports, hospitals, institutes and manufacturing and industrial facilities.

The commercial buildings segment is the largest market segment in 2016. Commercial buildings refer to office buildings and retail infrastructures such as malls and shopping stores. All these buildings have huge utilisation of energy and require high-tech security systems. As a result, they have a greater need for automated systems. This segment is expected to continue to dominate the market throughout the forecast period, with increasing energy-saving concerns expected to drive growth in the segment.

The market is also segmented along automation lines, services types and geographical regions.

In terms of automation class, the market is segmented into energy management, intelligent security systems, infrastructure management and network and communication management.

With regard to services, the market is segmented into professional services and managed services. The professional services segment constituted a major market segment in 2017. Demand is high for professional services such as consultation and training activities.

In developing regions, the smart building market is growing at a rapid pace. Accelerating technological developments and the adoption of new infrastructure security and services in emerging countries coupled with a hike in smart building programmes in these countries will propel the growth of the market in the Asia Pacific region. While Europe will continue to dominate, Asia Pacific is anticipated to take up a bigger slice of the pie in the forecast period.

The major market players in the smart building market are Siemens AG, ABB Group, Cisco Systems, Schneider Electric SE, United Technologies Corporation, BuildingIQ, Inc., Honeywell International, IBM, Johnson Controls and Delta Controls. SST

LOCKING THE DIGITAL FRONT DOOR

►► **By Kuei-Huan Chen,**
Senior Manager of Network Division, Synology Inc.

While smart home devices have been available to consumers for quite a while now, the rising capabilities and popularity of voice assistants has arguably been the strongest driver pushing the concept of the smart home into the mainstream. These voice assistants now reside on almost every consumer smartphone, which means that many consumers are now highly familiar with how they work and what they can do.

It is predicted by IDC that the smart home market will total nearly 1.3 billion devices by 2022, with the fastest growing category being the smart speakers segment, which includes voice assistants. Meanwhile Cisco forecasts that by 2020, the average home will contain more than 35 connected devices. From smart lighting to smart air conditioners, smart locks and even smart toilets, the smart home revolution promises to dramatically change how consumers think about their homes.

At the same time, many are savvy enough to recognise that such connectivity comes with increased cybersecurity risk. In the former age of the PC, when the computer was the only connected device most consumers owned, it was sufficient to install an antivirus and call it a day as far as securing your connected device is concerned.

Today, however, the exponentially larger number of connected devices also mean additional points of entry for hackers and increased digital security risk. Hacked devices present a wide range of risks, including the threat of being used to spy on their owners and even used to perform distributed denial-of-service (DDoS) attacks against other targets.

In the IDC report mentioned earlier, the market intelligence firm also notes that privacy and security are among the biggest factors holding back consumer adoption of smart home devices. Nevertheless, IDC predicts that consumers will find that the convenience these devices offer outweighs the security risks.

How then can consumers ensure that they stay safe while still enjoying the benefits of a smart home?

The Humble Router And Its Role In Digital Home Security

Many think of their routers as purely utilitarian devices. Consumers ponder whether their routers can support the bandwidth they pay their Internet Service Providers (ISPs) for, how fast the WiFi speed is, and whether the WiFi signal will be able to reach every corner of their home. Yet few ever worry about the security risk residing in the humble router. This is despite the fact that the router is the gateway through which all internet traffic in the house, including to and from connected devices, must traverse – including cyber attacks.

Consumers should be paying significantly more attention to their routers if they want to stay safe in the age of the Internet of Things (IoT). At the most basic level, it is critical to choose routers that feature frequent patch updates since hackers are constantly evolving their mode of cyber attacks, making it essential that consumers ensure that their defence line stays ahead of attacks.

There are security measures that can prevent the interception of wireless data. For example, security protocols enhance network protection against snooping and other attacks. As such, routers that feature the latest WPA3 certification – which was launched by the Wi-Fi Alliance – are good picks.

Monitoring your web traffic can also be enormously useful in spotting cybersecurity breaches. An abnormal increase in web traffic might indicate the presence of ransomware, while spikes in web traffic at a time when the household is asleep may mean that connected devices in your house are being controlled or used by outside parties.

Additional security features offered by some routers also include protection from malicious websites with built-in Google Safe Browsing integration and a constantly updated database, as well the ability to automatically inspect incoming and outgoing web traffic and drop any malicious packets detected.

Though more frequently used by business users in the past, router vendors are now focusing on making user interfaces more intuitive and easily understood. These can even be accessed with the use of mobile apps, allowing users to guard their smart homes even when they're not physically present.

Additional security features offered by some routers also include protection from malicious websites with built-in Google Safe Browsing integration and a constantly updated database, as well the ability to automatically inspect incoming and outgoing web traffic and drop any malicious packets detected.

User Habits Need Spring Cleaning Too

Simply getting a secure router isn't a cure-all for cybersecurity issues. Just as you should pick routers from vendors that offer frequent patch updates; the same advice applies to all connected devices you purchase. Frequently check vendor websites for these updates; some companies may not automatically push out these updates to users, making manual checking necessary.

Many consumers would also be familiar with this piece of advice, but it's important enough to bear repeating: practise good password hygiene. Change the default passwords on your devices – including routers and smart devices – as soon as possible, and make it a habit to change these passwords regularly. Last but not least, avoid using the same password across all your devices.

The benefits of the smart home are clear, and many consumers stand to benefit enormously as long as they recognise the risks and take the appropriate cybersecurity measures. These aren't as onerous as many people think. Basic tips include choosing your routers and connected devices wisely and practising good password hygiene. SST

96% of Singaporean Businesses Breached In Past Year, Reveals Carbon Black Report

A survey of Singapore enterprises conducted in January 2019 uncovered alarming findings: 96% of the organisations surveyed experienced regular security breaches.

Commissioned by leader in cloud-delivered, next-generation endpoint security firm Carbon Black, the report surveyed 250 Singaporean CIOs, CTOs and CISOs from companies of different organisation sizes and IT team sizes in industries including financial, healthcare, government, retail, manufacturing, food and beverage, oil and gas, professional services and media and entertainment.

The analysis paints a picture of a cyber defence landscape in Singapore that is under siege by increasingly sophisticated cyber attacks that are increasing in volume.

Among the key survey research findings:

- 96% of surveyed Singaporean organisations reported having been breached in the last 12 months
- the average number of reported breaches per surveyed organisation is 3.98
- 92% of surveyed organisations said they have seen an increase in attack volumes
- 95% of surveyed organisations said attacks have become more sophisticated
- 97% of surveyed organisations plan to increase spending on cyber defence

Ransomware is the most prolific attack type in Singapore according to the survey, with 28% of organisations surveyed naming it as the most frequently encountered. Malware and Google Drive (cloud data breach) were in second and third place at 25% and 11% respectively.

The human factor played a big part in the attacks that led to breaches, the survey found. Phishing attacks were at the root of 14% of successful breaches, the survey noted. Process weakness was the identified cause in 12% of breaches, according to the survey, indicating that basic security hygiene should be a priority for organisations.

Financial Institutions Face Increasingly Sophisticated Attacks

The survey found that financial institutions witnessed the greatest growth in attack sophistication with 63% reporting that attacks had grown increasingly sophisticated.

Nearly two-thirds of businesses in the manufacturing and engineering industry have been breached three to five times in the last 12 months, the survey found. Third-party applications and ransomware pose the greatest threats to this sector (both 23%), as these tactics were the primary causes of successful breaches, the survey found.

Threat Hunting Delivers On Its Promise

Fortunately, 79% of surveyed Singaporean organisations said they are actively threat hunting, with over a third (34%) having threat hunted for more than one year, the survey found. Nearly half (46%) said they started in the past year. A very encouraging 94% of those organisations reported that threat hunting has strengthened their defences and 41% said that it has significantly strengthened their defences.

"Our first Singaporean threat reported indicates that organisations in Singapore are under intense pressure from escalating cyber attacks," said Rick McElroy, Head of Security Strategy for Carbon Black. "The research indicates increases across the board in attack volume and sophistication, causing frequent breaches. In response, an encouraging number of Singaporean organisations are adopting threat hunting and seeing positive results. As threat hunting strategies start to mature, we hope to see fewer attacks making it to full breach status." SST

IBM Study: Over 50% Of Companies Fail To Test Their Cybersecurity Incident Response Plans

A global study by IBM Security reveals that a vast majority of organisations are still unprepared when it comes to responding to cybersecurity incidents. Among the findings: 77% of respondents do not have a cybersecurity incident response plan applied consistently across the enterprise.

Of the organisations surveyed that do have a plan in place, more than half (54%) do not test their plans regularly, which can leave them less prepared to effectively manage the complex processes and coordination that must take place in the wake of an attack.

This is despite studies showing that companies that can respond quickly and efficiently to contain a cyber attack within 30 days save over $1 million on the total cost of a data breach on average.

IBM Security offers enterprise security products and services. The global survey conducted by the Ponemon Institute on behalf of IBM features insight from more than 3,600 security and IT professionals from around the world, including the United States, Canada, United Kingdom, France, Germany, Brazil, Australia, Middle East and Asia Pacific. This is IBM Security's fourth annual benchmark study on cyber resilience.

These shortfalls in proper cybersecurity incident response planning have remained consistent over the past four years of the study.

The difficulty cybersecurity teams are facing in implementing a cybersecurity incident response plan has also impacted businesses' compliance with the General Data Protection Regulation (GDPR). Nearly half of the respondents (46%) said their organisation has yet to realise full compliance with GDPR, even as the one-year anniversary of the legislation quickly approaches.

"Failing to plan is a plan to fail when it comes to responding to a cybersecurity incident. These plans need to be stress tested regularly and need full support from the board to invest in the necessary people, processes and technologies to sustain such a programme," said Ted Julian, Vice President of Product Management and Co-Founder, IBM Resilient. "When proper planning is paired with investments in automation, we see companies able to save millions of dollars during a breach."

Other Key Findings

The 2018 Cost of A Data Breach Study also finds that:

- Automated response is still in the works. Less than one-quarter of the respondents said their organisation significantly uses automation technologies, such as identity management and authentication, incident response platforms and security information and event management tools, in their response process.

Photo credit: John Mottern

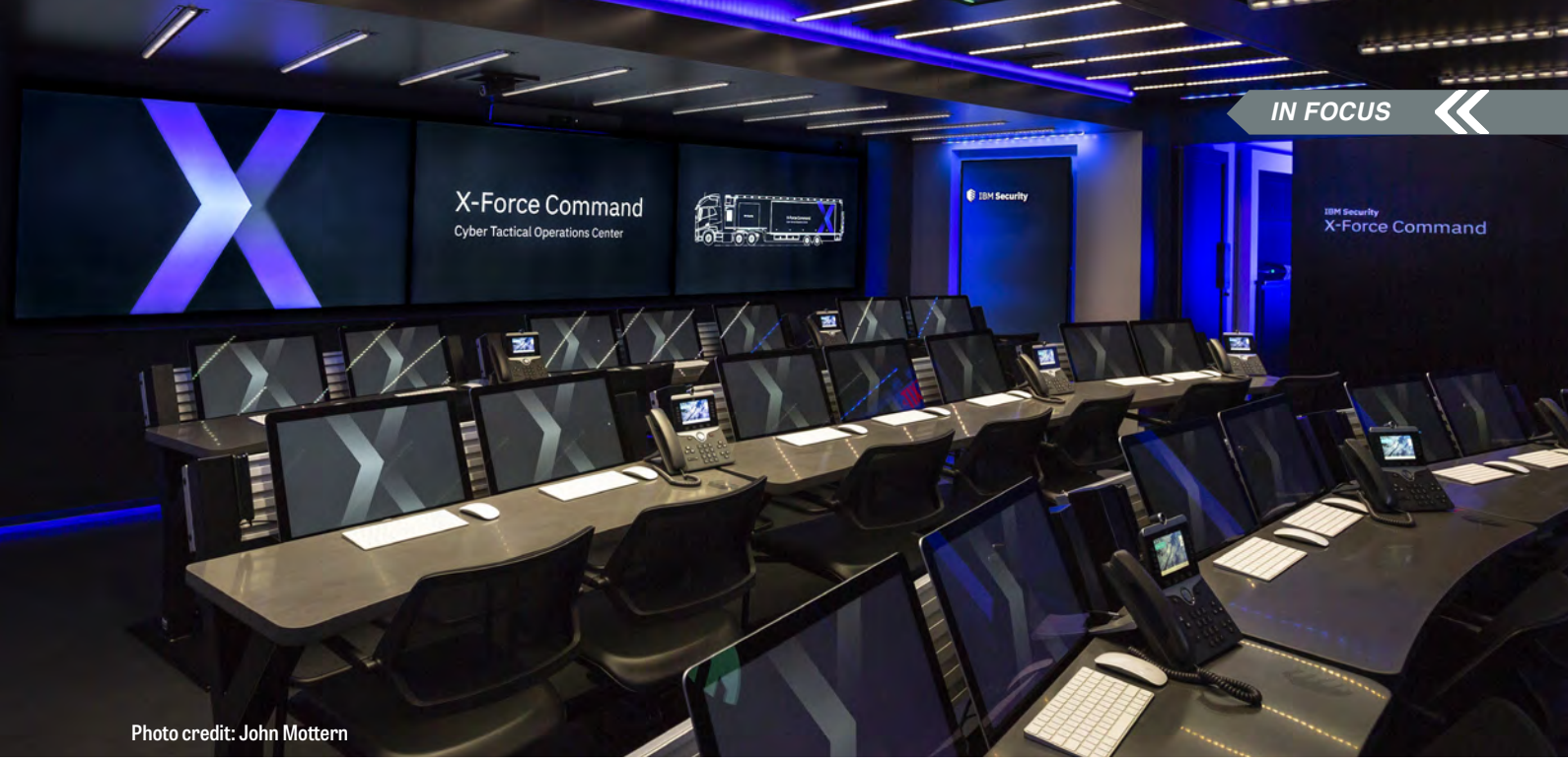


Photo credit: John Mottern

- Talents on the payroll are still inadequate to the task. Only 30% of respondents reported that staffing for cybersecurity is sufficient to achieve a high level of cyber resilience.

- Privacy and cybersecurity remain tied at hip. Many respondents (62%) indicated that aligning privacy and cybersecurity roles is essential or very important to achieving cyber resilience within their organisation.

Automation Still Emerging

For the first time, the study measured the impact of automation on cyber resilience. Automation refers to enabling security technologies that augment or replace human intervention in the identification and containment of cyber exploits or breaches. These technologies depend upon artificial intelligence, machine learning, analytics and orchestration.

When asked if their organisation leveraged automation, only 23% of respondents said they were significant users, whereas 77% reported their organisations only use automation moderately, insignificantly or not at all. Organisations with the extensive use of automation rate their ability to prevent (69% vs. 53%), detect (76% vs. 53%), respond (68% vs. 53%) and contain (74% vs. 49%) a cyber attack as higher than the overall sample of respondents.

The use of automation is a missed opportunity to strengthen cyber resilience, as organisations that fully deployed security automation saved $1.5 million on the total cost of a data breach when compared with organisations that did not leverage automation that suffered a much higher total cost of a data breach.

Skills Gap Still Impacting Cyber Resilience

The cybersecurity skills gap appears to be further undermining cyber resilience, as organisations reported that a lack of staffing hindered their ability to properly manage resources and needs. Survey participants stated they lack the headcount to properly maintain and test their incident response plans and are facing 10-20 open seats on cybersecurity teams. In fact, only 30% of respondents reported that staffing for cybersecurity is sufficient to achieve a high level of cyber resilience. Furthermore, 75% of respondents rate their difficulty in hiring and retaining skilled cybersecurity personnel as moderately high to high.

Adding to the skills challenge, nearly half of respondents (48%) said their organisation deploys too many separate security tools, ultimately increasing operational complexity and reducing visibility into overall security posture.

Privacy Growing As A Priority

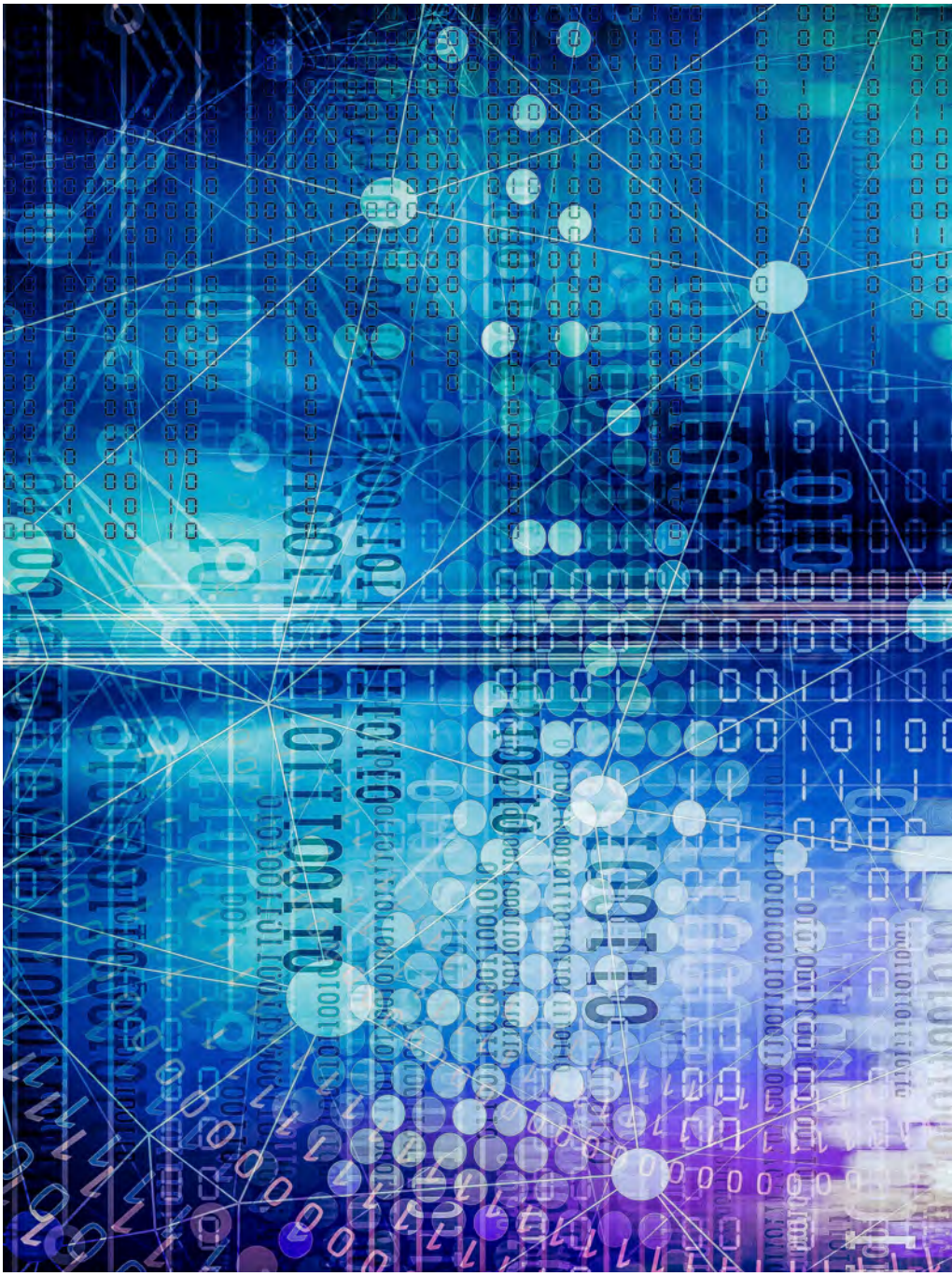
Organisations are finally acknowledging that collaboration between privacy and cybersecurity teams can improve cyber resilience, with 62% indicating that aligning these teams is essential to achieving resilience. Most respondents believe the privacy role is becoming increasingly important, especially with the emergence of new regulations like GDPR and the California Consumer Privacy Act, and are prioritising data protection when making IT buying decisions.

When asked what the top factor was in justifying cybersecurity spend, 56% of respondents said information loss or theft. This rings especially true as consumers are demanding businesses do more to actively protect their data. According to a recent survey by IBM, 78% of respondents say a company's ability to keep their data private is extremely important, and only 20% completely trust organisations they interact with to maintain the privacy of their data.

In addition, most respondents also reported having a privacy leader employed, with 73% stating they have a Chief Privacy Officer, further proving that data privacy has become a top priority in organisations. SST

Study Reveals Evolving Asia Pacific Cybersecurity Landscape

The 2019 DomainTools and Ponemon study on automation and cybersecurity staffing in Asia Pacific, United States and the UK reveals an evolving Asia Pacific cybersecurity arena.



More than 1,400 security professionals based across the Asia Pacific (APAC), US and the UK were surveyed for the Staffing the IT Security Function in the Age of Automation study. All respondents in the study are responsible for attracting, hiring, promoting and retaining cybersecurity personnel within their organisations. In the study, they revealed their concerns regarding the adoption of automation and AI as cybersecurity tools.

DomainTools is a leader in domain name and DNS-based cyber threat intelligence, while the Ponemon Institute is a research centre dedicated to privacy, data protection and information security policy.

A Skill Shortage Across All 3 Geographical Regions

The study showed a clear shortage of cybersecurity staff across all the geographical regions surveyed, with 78% of all respondents admitting their teams are understaffed.

According to respondents, automation will partially solve the problem, relieving cybersecurity professionals of time-consuming and non-cost-effective tasks such as malware analysis, which is either already automated (50%), or is to become so in the next three years (56%). Only 35% of respondents, however, think that

automation will reduce the headcount of their cybersecurity function: 40% even expect an increased need for hires with more advanced technical skills.

Dr. Larry Ponemon, chairman and founder of the Ponemon Institute

"Within just one year, the perspective around adoption of automated technologies has notably shifted among cybersecurity professionals," said Dr. Larry Ponemon, chairman and founder of the Ponemon Institute. "Contrary to the popular belief that the rise of automation will threaten the job market, organisations now feel these technologies will help ease the current strain on resources, and offer the potential to promote job security for highly skilled staff, while strengthening cybersecurity defences."

UK and US respondents were much more confident that automation will improve their cybersecurity staff's ability to do their job (59% and 65% of respondents respectively) than Asia Pacific respondents (48%), who were also more likely to distrust AI as a cybersecurity tool (37% of respondents, compared to 31% in the UK and 24% in the US).

Asia Pacific Ahead In Cybersecurity Skills Availability

Skills shortages also seemed to be lower in Asia Pacific (67%) compared to the UK (70%) and the US (78%), perhaps partially explaining the different level of reliance and trust on automation and AI across regions. At the same time, the survey reported that 40% of respondents expect an increased need for hires with more advanced technical skills, especially in Asia Pacific where governments and educational institutions are already accelerating specialised cybersecurity programmes and initiatives, such as the ASEAN-Singapore Cybersecurity Centre of Excellence announced during the Asean Ministerial Conference on Cybersecurity in September 2018, with ASEAN nations adopting a rules-based approach to regional cybersecurity frameworks.

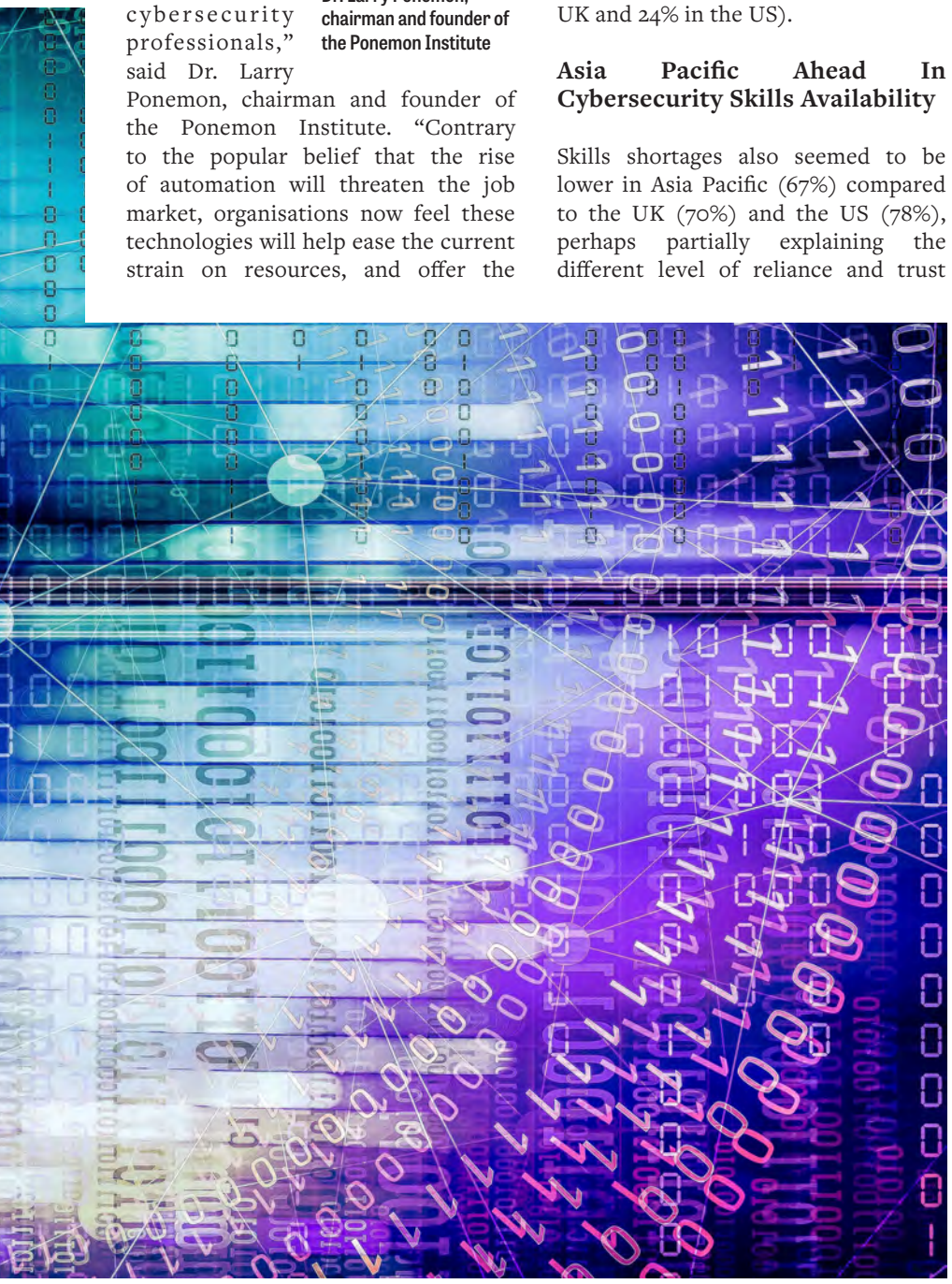
ASEAN, or the Association of Southeast Asian Nations, is a 10-nation group comprised of Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, the Philippines, Singapore, Thailand and Vietnam.

Of those respondents who said AI is trusted as a security tool in their organisations, the majority listed staff shortages as the main reason why their enterprise has adopted the solution (53%).

Corin Imai, senior security advisor at DomainTools

"The results of the survey reveal that, overall, cybersecurity professionals are confident that automation will make their workload more manageable and will increase the accuracy of certain tasks, without jeopardising their job security," said Corin Imai, senior security advisor at DomainTools.

"Although there are geographical differences in the level of confidence placed in AI and automation as cybersecurity tools, the reasons that motivate their adoption – relieving overworked teams, preventing downtime and business disruptions, reducing threats created by operating in the global digital economy, etc. – seem to be consistent across regions, suggesting that goals and expectations are aligned for organisations across the globe." SST



Cybercriminals Attack Cloud Server Honeypot Within 52 Seconds, Reports Sophos

According to Sophos's latest global report **Exposed: Cyberattacks on Cloud Honeypots,** cloud server honeypots across 10 global locations are attacked within 40 minutes on average.

A honeypot is a system intended to mimic likely targets of cyber attackers to allow security researchers to monitor cybercriminal behaviours. The honeypots were set up in 10 of the most popular Amazon Web Services (AWS) data centres in the world, including California, Frankfurt, Ireland, London, Mumbai, Ohio, Paris, Sao Paulo, Singapore and Sydney over a 30-day period.

The report revealed that cloud servers were subjected to 13 attempted attacks per minute, per honeypot, on average. More than 5 million attempted attacks were recorded on all cloud server honeypots in a 30-day period. In fact, cybercriminals attacked one of the cloud server honeypots in the study within 52 seconds of the honeypot going live in Sao Paulo, Brazil. Released in April 2019, the study reveals the need for visibility and security to protect what businesses put into hybrid and all-cloud platforms.

Sophos, a global leader in network and endpoint security, describes the activities as demonstrating how cybercriminals are automatically scanning for weak open cloud buckets. Cybercriminals also use breached cloud servers as pivot points to gain access to other servers or networks.

"The aggressive speed and scale of attacks on the honeypots shows how relentlessly persistent cybercriminals are and indicates they are using botnets to target an organisation's cloud platforms," said Matthew Boddy, a security specialist at Sophos. "The issue of visibility and security in cloud platforms is a big business challenge, and with increased migration to the cloud, we see this continuing."

Visibility Into Weaknesses

Continuous visibility of public cloud infrastructure is vital for businesses to ensure compliance and to know what to protect. However, multiple development teams within an organisation and an ever-changing, auto-scaling environment make it problematic to secure data.

Sophos seeks to address this security weaknesses in public clouds by launching Sophos Cloud Optix, which leverages artificial intelligence to highlight and mitigate threat exposure in cloud infrastructures.

Sophos Cloud Optix is an agentless solution that provides intelligent cloud visibility, automatic compliance regulation detection and threat response across multiple cloud environments. Sophos Cloud Optix leverages AI-powered technology from Avid Secure, which Sophos acquired in January 2019. Founded in 2017 by a team of highly distinguished leaders in IT security, Avid Secure revolutionised the security of public cloud environments by providing effective end-to-end protection in cloud services, such as AWS, Azure and Google.

Instead of inundating security teams with a massive number of undifferentiated alerts, Sophos Cloud Optix significantly minimises alert fatigue by identifying what is truly meaningful and actionable. In addition, with visibility into cloud assets and workloads, IT security teams can have a far more accurate picture of their security posture that allows them to prioritise and proactively remediate the issues flagged in Sophos Cloud Optix.

Key features in Sophos Cloud Optix include:

Smart Visibility: It enables automatic discovery of an organisation's assets across AWS, Microsoft Azure and Google Cloud Platform (GCP) environments, via a single console, allowing security teams complete visibility into everything they have in the cloud and to respond to and remediate security risks in minutes.

Continuous Cloud Compliance: It helps security teams keep up with continually changing compliance regulations and best practices policies by automatically detecting changes to cloud environments in near-time.

AI-Based Monitoring and Analytics: It shrinks incident response and resolution times from days or weeks to just minutes.

"The AI-powered monitoring and alerts helped reduce the noise and allowed our teams to focus on delivering value to the business," said Aaron Peck, vice president and CISO, Shutterfly, Inc., a Sophos customer based in Redwood City, California. SST

Smart City Solutions Week 2019
28-31 October 2019,
Bangkok International Trade & Exhibition Centre,
Bangkok, Thailand

Smart City Solutions Week Debuts In Thailand

There is a new destination for seekers of smart city solutions with the launch of Smart City Solutions Week in Thailand in October 2019.

Messe Frankfurt, the world's largest trade fair, congress and event organiser, will join forces with Digital Economy Promotion Agency (DEPA) to stage the inaugural event from 28 to 31 October 2019.

An ensemble of four shows, the event will gather three of Messe Frankfurt's existing shows for the smart city industry - Secutech Thailand, Thailand Lighting Fair and Thailand Building Fair – together with the DEPA-organised Digital Thailand Big Bang show, which will focus on digital infrastructure. Collectively the four shows will serve as a one-stop shop for the latest smart city technology and solutions.

The 2018 edition of Secutech Thailand, Thailand Lighting Fair and Thailand Building Fair drew 300 exhibitors from 18 countries and regions and over 10,000 visitors. With a new show date and a new enlarged format with the addition of Digital Thailand Big Bang, it is forecast that Smart City Solutions Week 2019 will see bigger visitor numbers.

What You Can Expect At The Fair

Secutech Thailand will showcase the latest AI and IoT security innovations for the smart city including the latest surveillance systems, biometric identification systems, smart sensors, alarms, access control systems and crowd management systems. The show space will be divided into five zones: Smart Police Zone, Safe Factory Zone, Smart Transportation Zone, Smart Campus Zone and Smart Solutions Zone for Waste and Environment Management.

Thailand Lighting Fair and Thailand Building Fair will present the full spectrum of the smart city concept including digital applications (smart lighting solutions, smart parking and smart buildings), smart technology (intelligent sensors, dimming and control and smart lighting platforms) and smart governance (facility management and smart community features).

Digital Thailand Big Bang will showcase the ways in which big data can be used to transform society and improve urban living standards, including city management systems, cloud computing, fintech products and digital infrastructure such as submarine cables and satellites.

Located at the Bangkok International Trade & Exhibition Centre, Secutech Thailand and Digital Thailand Big Bang will be held from October 28 - 31, while Thailand Lighting Fair and Thailand Building Fair will be held from October 28 - 30.

Said Hubert Duh, Chairman and Managing Director, Messe Frankfurt New Era Business Media Ltd, "The synergy created amongst the four fairs will not only enhance the visitor experience but also help to build even more momentum for ASEAN's smart city sector."

Remarked Dr. Nuttapon Nimmanphatcharin, President and CEO of DEPA, "The adoption of the smart city concept is an undeniable trend for ASEAN cities and we hope that industry players will take advantage of these integrated solutions and build a networking platform across the smart city ecosystem." SST

BMAM Expo Asia 2019
27 - 29 June 2019
IMPACT Exhibition and Convention Centre,
Bangkok, Thailand

Enjoy BMAM Expo Asia 2019 And K-Fire & Safety Bangkok 2019 In One Show!

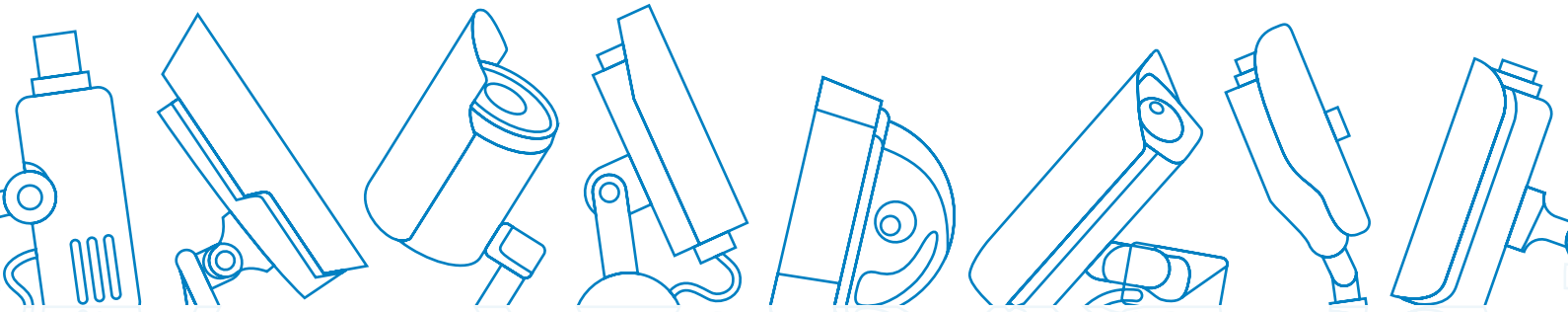
The 12th edition of BMAM Expo Asia 2019 will take place in Bangkok this June.

This leading building and facilities management event is expected to attract more than 150 exhibitors and 4,000 facilities management professionals and key decision makers from the region.

Featuring cutting-edge solutions and a leading industry knowledge platform for facilities management, the trade exhibition will be held from 27 to 29 June 2019 in Hall 6 of IMPACT Exhibition Center, Bangkok, Thailand.

For the first time, the edition is co-located with K-Fire & Safety Expo Bangkok 2019, Korea's leading international exhibition on fire and safety. This means that expo visitors can also discover the latest fire and safety solutions (including fire vehicles, fire hoses, fire extinguishers, fire cloths and fire detectors) offered by more than 30 companies taking up the 100 booths from the Republic of Korea.

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 CONSTRUCTION · Security Solutions Today · bathroom+kitchen today · lighting today

GET IT ON Google Play

Download on the App Store

More Than Just An Exhibition

BMAM Expo Asia is the meeting point for the facilities management industry.

One of the biggest draws is the Building & FM Conference, which will address how technology disruption is driving the transformation of the facilities management industry.

In addition, there will be a series of conferences, seminars and workshops that will run alongside the exhibition. These happenings focus on three key themes: facilities management products and services, green facilities management and smart building solutions.

BMAM Expo Asia will also feature a Dealer & Distributor Tour designed to allow dealers and distributors to tour exhibitors that are seeking new distribution channels. This tour is organised in collaboration with industry associations, including the Asia Pacific Security Association, RFID & IoT Association, Smart Cities Thailand Association, Thailand Cleaning Contractors' Club and BIM Club Thailand.

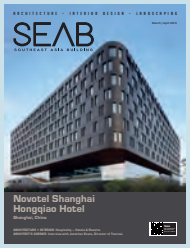
Finally, the BSA Building Safety Awards recognise organisations with the best building safety records, while the Consultancy Clinic offers building owners the opportunity to meet leading consultants for comprehensive information and advice on building and facilities management. SST

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

Robert Bosch	Singapore	+65 6258 5511	enquiry.apr@sg.bosch.com	www.boschsecurity.com	OBC
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

Avigilon	U.S.A.	+1 888 281 5182	asksales@avigilon.com	www.avigilon.com	7

See us at following upcoming events!

Event	Date	City	Country	Website	Page
Secutech 2019	8 – 10 May 2019	Taipei	Taiwan	www.secutech.com	13
IFSEC International 2019	18 – 20 Jun 2019	London	United Kingdom	www.ifsec.events/international	IBC
IFSEC Philippines 2019	13 – 15 Jun 2019	Manila	Philippines	www.ifsec.events/philippines	9
BMAM Expo Asia 2019	27 – 29 Jun 2019	Bangkok	Thailand	www.bmamexpoasia.com	11
INTERPOL World 2019	2 – 4 July 2019	Singapore	Singapore	www.interpol-world.com	1
Secutech Vietnam 2019	14 – 16 Aug 2019	Ho Chi Minh City	Vietnam	www.secutechvietnam.com	21
Bex Asia 2019	4 – 6 Sept 2019	Singapore	Singapore	www.bex-asia.com	15
Safety & Security Asia 2019	1 – 3 Oct 2019	Singapore	Singapore	www.safetysecurityasia.com.sg	17
Secutech Thailand 2019	28 – 31 Oct 2019	Bangkok	Thailand	www.secutechthailand.com	19

BOSCH
Invented for life

Secure operations 24/7 to see all the details, all the time with Bosch FLEXIDOME IP starlight 8000i.

With quick installation plus wireless and remote commissioning, camera adjustments can be corrected whenever needed plus up to 4k Ultra HD resolutions and starlight technology so you can see all the details all the time.

Find out more at **boschsecurity.com**