JAN / FEB 2020

SECURITY SOLUTIONS TODAY

FUNDAMENTALS OF SMART BUILDINGS

Keeping smart buildings secure and safe from threats and vulnerabilities

Lite yet competitive

Dahua Leading NVR4000-4KS2/L Series

- Affordable solution with IP Cameras suitable for Home, Villa, Retail, etc.
- Supports front-end AI functions, such as SMD Plus, Perimeter Protection, People Counting, and Heat Map.
- The brand new GUI design enables easy system operation.

Recommended Models

NVR4104-P-4KS2/L

NVR4108HS-8P-4KS2/L

NVR4216-4KS2/L

NVR4216-16P-4KS2/L

CE FC RoHS 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

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

IN THIS ISSUE

ZETTLER

Earlier Detection.
Fewer False Alarms.

ZETTLER makes it possible. For building owners, a single false alarm can cause big problems. Only ZETTLER combines PROFILE Flexible panels with 3oTec 850PC triple-sensing detectors to monitor smoke, heat and CO levels simultaneously – reducing false alarms while providing earlier detection. Backed by approvals from across Europe, ZETTLER leads the way in faster, more accurate fire detection. Because protecting life matters. And safety should never be a compromise.

For more information about ZETTLER PROFILE and 3oTec 850PC products, visit **zettlerfire.com**

Johnson Controls

CONTACT

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

EDITOR
CJ Chia
(sst@tradelinkmedia.com.sg)

ASSOCIATE PUBLISHER
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)

Vectors Credit: Freepik.com

Designed by Fawzeeah Yamin

SECURITY SOLUTIONS TODAY
is published bi-monthly by
Trade Link Media Pte Ltd (Co. Reg. No.: 199204277K)
101 Lorong 23, Geylang,
#06-04, Prosper House, Singapore 388399
Tel: +65 6842 2580 Fax: +65 6842 2581
MCI (P) 084/05/2019 | ISSN 2345-7104 (Print)

Printed in Singapore by
Fuisland Offset Printing (S) Pte Ltd

ANNUAL SUBSCRIPTION:

Surface Mail:	
Singapore	- S$60 (Reg No: M2-0108708-2 Incl. 7% GST)
Airmail:	
Malaysia/Brunei	- S$105
Asia	- S$155
Japan, Australia, New Zealand	- S$185
America/Europe	- S$185
Middle East	- S$185

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

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

ISSN 2345-7104
9 772345 710005

MicroEngine®

Integrated Security Systems

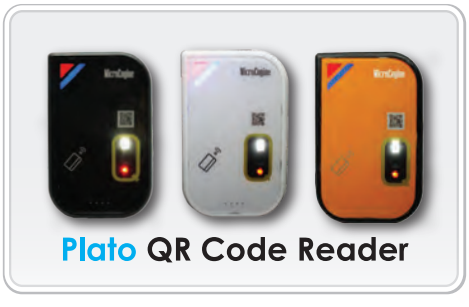
The Trusted Brand in Security Solutions

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

MAR 18 – 20 2020

SECON 2020
Seoul, South Korea
+82 2 6715 5400 www.seconexpo.com
global@seconexpo.com

MAR 18 – 20 2020

ISC West 2020
Las Vegas, USA
203 840 5602 www.iscwest.com
www.iscwest.com/Forms/Customer-Service-Form/

MAR 19 – 22 2020

Megabuild 2020
Jakarta, Indonesia
+62 21 2556 5022 www.megabuild.co.id
megabuild@reedpanorama.com

APR 22 – 24 2020

Secutech 2020
Taipei, Taiwan
+886 2 8729 1017, +886 2 8729 1099 www.secutech.tw.messefrankfurt.com/taipei/en.html
kirstin.wu@newera.messefrankfurt.com, services@secutech.com

MAY 07 – 09 2020

Secutech India 2020
Mumbai, India
+91 22 4286 3869 www.secutechexpo.com
info@secutechexpo.com, info@firesafetyexpo.in

MAY 19 – 21 2020

IFSEC International 2020
London, UK
+44 (0)20 7069 5000 www.ifsec.events/international/
ifseccustomerservice@ubm.com

JUN 23 – 25 2020

IFSEC Southeast Asia 2020
Kuala Lumpur, Malaysia
+60 3-0771 2688 www.ifsec.events/kl/
ifseccustomerservice@ubm.com

JUL 22 – 24 2020

IFSEC Philippines 2020
Manila, Philippines
+63 2 551 7718 www.ifsec.events/philippines/
www.ifsec.events/philippines/eform/submit/contact

AUG 20 – 22 2020

Secutech Vietnam 2020
Ho Chi Minh City, Vietnam
+886 2 8729 1099, +84 4 3936 5566 www.secutechvietnam.tw.messefrankfurt.com
stvn@newera.messefrankfurt.com, project1@vietfair.vn

SEP 21 – 23 2020

Global Security Exchange 2020
Atlanta, USA
+1 888 887 8072, +1 972 349 7452 www.gsx.org
asis@asisonline.org

secutech
INDIA

Find effective pathways into Asia's fastest growing market

07 – 09 May 2020
Bombay Exhibition Centre
Goregaon (E) Mumbai India

www.secutechindia.co.in

ABEC

messe frankfurt

Dear readers,

Many cities globally have planned roadmaps that lead to smart cities. As the building blocks of the ecosystem for a smart city, it's essential to look at each smart building and understand what it brings to the table.

With automation and smart technology on the rise, smart buildings are an inevitable part of the future. Buildings that can detect when a room is not in use and turn off the air conditioning and lights automatically are more energy efficient, while integrated security systems help to keep a building's occupants safe.

As great as it all sounds, the technology also opens the door for new vulnerabilities that are unique to smart buildings. In our cover story, we look at how smart buildings enhance security, the unique vulnerabilities and the threats that must be kept in mind, as well as possible solutions to reduce the risk of cyberattacks.

In this issue, we also take a glimpse into how retail and hospitality are changing in the age of increased connectivity; as technology becomes ever smarter, the definition of a great customer experience is changing, and the customer journey needs to be updated to match new expectations.

In addition, we dive into how integrated access control and key management systems have changed and will continue to evolve, and check out the security considerations that you might have if you're thinking of moving your data to the cloud.

As we start a brand new year, we look forward to exciting new developments in the world of security, and with it, the opportunity to bring you the latest updates on technological and security advancements.

Happy reading!

CJ Chia

Editor

Part of the
ASEAN Super 8 Series

IFSEC SOUTHEAST ASIA

SECURITY • FIRE • SAFETY

23 - 25 JUNE 2020

MALAYSIA INTERNATIONAL TRADE AND EXHIBITION CENTRE (MITEC), KL

SECURITY IS CRITICAL
IFSEC IS ESSENTIAL

Organised By
informa markets | UBM

WWW.IFSECSEA.COM

@IFSECSEA #IFSECSEA IFSEC Southeast Asia

MICROSOFT INCREASES DATA PROTECTION FOR ENTERPRISES FOLLOWING DUTCH MOJ AUDIT

Microsoft has made privacy changes related to Office 365 following an audit 12 months ago for the Dutch justice ministry, which raised concerns over data leaks.

Previously, an audit conducted by Privacy Company for the Dutch Ministry of Justice and Security recommended disabling any settings in Microsoft Office 2016 that send data to Microsoft servers.

A report on Reuters in August 2019 noted that tests carried out by the Dutch Data Protection Authority (DPA) revealed that Microsoft was remotely collecting data from users. "As a result, Microsoft is still potentially in breach of privacy rules," the DPA told Reuters.

In July 2019, the Dutch Ministry of Justice and Security approved measures taken by Microsoft to address the concerns raised in November 2018. On the technical side, feedback from the Dutch justice ministry and others led Microsoft to roll out a number of new privacy tools across its major services and make specific changes to Office 365 ProPlus, as well as increased transparency regarding use of diagnostic data.

Microsoft has now made an update to the privacy provisions in the Microsoft Online Services Terms (OST) in its commercial cloud. According to Julie Brill, corporate vice-president for global privacy and regulatory affairs and chief privacy officer at Microsoft, the updated OST reflects the contractual changes Microsoft developed with the Dutch ministry.

"Our updated OST will reflect contractual changes we have developed with one of our public sector customers, the Dutch Ministry of Justice and Security (Dutch MoJ). The changes we are making will provide more transparency for our customers over data processing in the Microsoft cloud," Brill wrote in a blog post.

"The only substantive differences in the updated terms relate to customer-specific changes requested by the Dutch MoJ, which had to be adapted for the broader global customer base. The work to provide our updated OST has already begun. We anticipate being able to offer the new contract provisions to all public sector and enterprise customers globally at the beginning of 2020," she wrote.

Brill said that under the European Union's (EU) General Data Protection Regulation (GDPR), Microsoft is recognised as a data processor, since the company collects and uses personal data from its enterprise services to provide online services requested by customers and for the purposes instructed by customers. Brill said this level of data stewardship has now been extended to enterprise services.

Microsoft may have needed to make the change as a result of intervention from the European Data Protection Supervisor (EDPS). In October 2019, the EDPS requested that Microsoft offer contractual changes such as those negotiated with the Dutch justice ministry to its customers in EU institutions.

At the time, Wojciech Wiewiórowski, assistant supervisor at the EDPS, said: "We are committed to driving positive change outside the EU institutions to ensure maximum benefit for as many people as possible. The agreement reached between the Dutch Ministry of Justice and Security and Microsoft on appropriate contractual and technical safeguards and measures to mitigate risks to individuals is a positive step forward."

The EDPS said it recognised that EU institutions outsource the processing of large amounts of personal data but highlighted that EU institutions still remain accountable for any processing activities carried out on their behalf. The EDPS said EU institutions must assess these risks and have appropriate contractual and technical safeguards in place to mitigate them. It recommended that all data controllers operating within the European Economic Area adopt similar contractual and technical safeguards.

"Through the OST update we are announcing we will increase our data protection responsibilities for a subset of processing that Microsoft engages in when we provide enterprise services," Brill wrote in the blog post.

"In the OST update, we will clarify that Microsoft assumes the role of data controller when we process data for specified administrative and operational purposes incident to providing the cloud services covered by this contractual framework, such as Azure, Office 365, Dynamics and Intune. This subset of data processing serves administrative or operational purposes."

IFSEC PHILIPPINES

SECURITY • FIRE • SAFETY

22 – 24 JULY 2020

SMX CONVENTION CENTER
PASAY CITY, METRO MANILA

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

Organised By
informa markets | UBM

WWW.IFSECPHILIPPINES.COM

@IFSECPH #IFSECPHILIPPINES IFSECPHILIPPINES

NANOLOCK SECURITY JOINS MEKOROT TO DELIVER CYBER PROTECTION FOR UTILITIES

NanoLock Security, the market leader of flash-to-cloud, powerful security solution for Internet of Things (IoT) and connected edge devices announced that it was joining forces with Israel's national water company, Mekorot, to develop cybersecurity solutions for water and energy utilities in Israel and around the world.

Due to the critical role that water and power infrastructure plays in our society and its increasing reliance on connected devices, utilities are an especially appealing target for multiple attack vectors, such as state-level outsider attacks, insider attacks from employees who have or were once granted access to device control, and even off-shore supply chain attacks. The possibilities for destruction are vast – from a disgruntled employee gaining access to a wastewater plant and changing settings that could cause contaminated water, to shutting down power for entire cities. To keep water and energy infrastructure safe, it is crucial that connected devices are protected throughout their entire lifecycle, starting at the production line and through the supply chain, field operation, and remote software updates, until end-of-life.

NanoLock Security developed an innovative security by design solution with a device level flash-to-cloud security protection, monitoring, and management solution, specifically developed for connected devices and IoT applications. The solution creates a hardware (HW) root-of-trust in the flash memory of the device that blocks all unauthorised code modifications, while moving the control from the vulnerable device to a trusted entity in the utility data centre. Since typical attacks manipulate the flash memory of the connected device to create persistency that survives reset, the HW root-of-trust protects the device's firmware and critical code (e.g. configuration, loggers, and boot), thus preventing malicious manipulation.

NanoLock's solution is processor and operating system agnostic and requires zero processing power or additional energy, making it perfectly suited for smart water and gas meters, which are battery-operated and very sensitive to power consumption.

"We are developing partnerships with companies like NanoLock to enable innovation in the delivery of the world's water. Essential to that mission is that utilities are protected from nefarious cyber threats and cities are safe from the consequences of attack," said David Balsar, GM of Mekorot Innovation and Ventures. "NanoLock's solution to secure IoT devices from within the flash memory is a technical innovation that we believe will help protect Israel's national water, as well as those utility ecosystem partnerships we have made across the globe"

"The time is now for decision-makers in the utilities industry to ensure cyber protection with a security by design approach, such as NanoLock's solution – one that is future-proof and scalable and can protect the world's critical infrastructure (including brownfield and legacy systems) for the long-term," said Eran Fine, CEO of NanoLock Security. "As a leading authority on water management, Mekorot has made a commitment to developing an ecosystem that delivers secure utilities, and they are working with us to put a global focus on cyber defence solutions for this market."

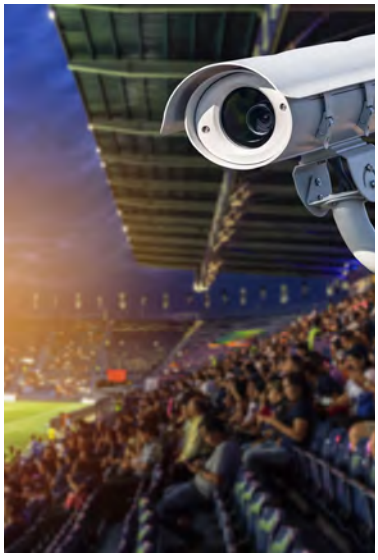
Through partnerships with the world's leading memory vendors, NanoLock secures seamless hardware root-of-trust that enables system integrators and device makers to ensure unprecedented protection, security, and control.

ISC WEST

PREMIER SPONSOR:
SIA
SECURITY INDUSTRY ASSOCIATION

CONNECTED SECURITY | DRONES & ROBOTICS | EMERGING TECH | LOSS PREVENTION & SUPPLY CHAIN | PUBLIC SAFETY | SMART HOME

SAVE THE DATE



COMPREHENSIVE SECURITY
FOR A SAFER,
CONNECTED WORLD

- Discover the industry's latest products, technologies & solutions
- Network with 30,000+ Physical, IoT and IT Security Professionals
- Direct access to 1,000 leading exhibitors & brands
- 85+ SIA Education@ISC Sessions

SIA EDUCATION@ISC:
MARCH 17-19, 2020

EXHIBIT HALL:
MARCH 18-20, 2020

SANDS EXPO, LAS VEGAS

Register today at:
ISCWEST2020.COM/TLM

#ISCWEST

RESEARCHERS COMPROMISE QUALCOMM "SECURE WORLD"

Up until now, Qualcomm's "Secure World" has been thought to be impenetrable. Accordingly, our credit and debit card information, along with other sensitive, personal information, saved onto our phones go directly into storage in Qualcomm's "Secure World". Through a 4-month research study, Check Point Research dispelled the belief that Qualcomm's "Secure World", which is dubbed by industry experts as the safest component of our mobile phones, is breach-proof by cyber hackers.

Check Point's research reveals that a gaping hole exists, uniquely enabling cyber hackers to steal our mobile payment information.

It is well known that pure software solutions have security limitations. Secure storage systems that are based on pure software mechanisms lack important hardware security features and, therefore, expose the data to a broader range of threats.

Android software by itself has the same security limitations, which Qualcomm addresses through hardware-based features. To address the limitation, the runtime of Android needs to be protected from both attackers and users. This is typically achieved by moving the secure storage software to a hardware supported Trusted Execution Environment (TEE).
Mobile operating systems, such as Android, offer a Rich Execution Environment (REE), providing a hugely extensive and versatile runtime environment. While bringing flexibility and capability, REE leaves devices vulnerable to a wide range of security threats. The TEE is designed to reside alongside the REE and provide a safe area on the device to protect assets and to execute trusted code.

The TEE on Qualcomm technology is based on ARM TrustZone technology. TrustZone is a set of security extensions on ARM architecture processors providing a secure virtual processor backed by hardware-based access control. This secure virtual processor is often referred to as the "secure world", in comparison to the "non-secure world", where REE resides. In 2018, it was documented that Qualcomm lead the processor market at 45% revenue share.

In a 4-month research project, Check Point researchers attempted and succeeded to reverse Qualcomm's "Secure World" operating system. Check Point researchers leveraged the "fuzzing" technique to expose the hole. Fuzz testing (fuzzing) is a quality assurance technique used to discover coding errors and security loopholes in software, operating systems or networks. It involves inputting massive amounts of random data, called fuzz, to the test subject in an attempt to make it crash.

Check Point implemented a custom-made fuzzing tool, which tested trusted code on Samsung, LG, Motorola devices. Through "fuzzing", Check Point found 4 vulnerabilities in trusted code implemented by Samsung (including S10), 1 in Motorola, 1 in LG, 1 related to LG, but all code sourced by Qualcomm itself. Hence, we proved that programmers of all best vendors and Qualcomm made mistakes in their code! Check Point Research urges mobile phone users to stay vigilant and check their credit and debit card providers for any unusual activity. In the meantime, we are working with the vendors mentioned to issue patches.

TREND MICRO DEBUTS BROADEST SECURITY SERVICES PLATFORM FOR BUILDING CLOUD APPLICATIONS

Trend Micro Incorporated, the global leader in cloud security, announced the launch of Trend Micro Cloud One™, a security services platform for organisations building applications in the cloud. Cloud One allows developers to rapidly build applications using the cloud services they want, while managing their organisation's risk.

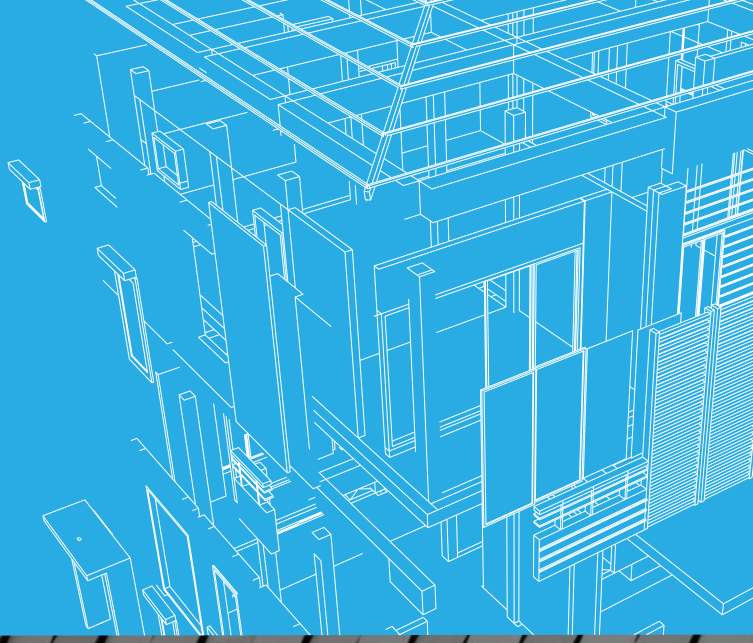
Cloud One delivers the industry's broadest range of security capabilities in a single platform. Designed to help organisations meet their most strategic cloud priorities, it allows customers to migrate existing applications to the cloud, deliver new cloud-native applications and achieve cloud operational excellence. The first-of-its-kind platform has the flexibility to solve immediate customer challenges and the innovation to rapidly evolve with cloud services.

At its heart, Cloud One includes the world's leading workload security service that is already in use by thousands of organisations. It is complemented by enhanced container security and brand-new offerings for application security, network security, file storage security and cloud security posture management to ensure cloud infrastructure is optimally configured.

Many cloud security solutions are often hard to manage and deploy, inflexible and fail to provide the level of visibility IT teams need to manage fast-emerging risks. Trend Micro's all-in-one platform approach is designed

To be continued on page 16

MEGABUILD
INDONESIA
2020



BE INSPIRED

19 - 22 MARCH 2020

JAKARTA CONVENTION CENTER

THE 19TH INDONESIA MOST COMPREHENSIVE BUILDING MATERIALS, DESIGN AND ARCHITECTURE EVENT

ROOF & FLOORING • BATHROOM & KITCHEN • CONSTRUCTION MATERIALS • DOORS & WINDOW • BUILDING MATERIALS • INTERIOR FURNISHING

PROGRAM & ACTIVITY MEGABUILD 2020

Seminar & Conference | Architecture Gallery | Trade Exhibitions | House of Indonesia Showcase

BOOK YOUR SPACE NOW!

CALL OUR REPRESENTATIVE

International Sales Manager

Ms. Astri Ratnasari

+62 811 9910 689

astri.ratnasari@reedpanorama.com

to deliver simplified, automated and flexible protection, regardless of where an organisation is on the journey to the cloud. Customers using the platform will benefit from a single-sign-on to all services, common user and cloud service enrolment, visibility from a single console, and a common pricing and billing model.

“We have been helping our customers with secure cloud transformation since the birth of the cloud, over a decade ago,” said Nilesh Jain, Vice President, Southeast Asia and India, Trend Micro. “Customers have a mix of legacy servers, virtualised data centres, and newer services such as containers and serverless applications, all of which can be protected using Cloud One.”

Trend Micro’s new cloud security platform supports the leading cloud providers, including Amazon Web Services (AWS), Microsoft Azure and Google Cloud.

“As more companies move their infrastructure and applications to the cloud, and adopt a shared responsibility model, we want our customers to have the option of the broadest choice from the best products in the market,” said Dave McCann, Vice President, AWS Migration, Marketplace and Control Services at Amazon Web Services, Inc. “Trend Micro’s new cloud security platform represents another example of new innovation, that is available via AWS Marketplace. By leveraging AWS Marketplace features like SaaS Contract API, Private Offers, and Consulting Partner Private Offers, customers can contract directly from Trend Micro, or their consulting partners around the world. We are committed to empowering our shared customers with easy and fast procurement and provisioning.”

Organisations like Armor in Dallas, Texas, are relying on Trend Micro for strategic cloud security.

CISCO EARNINGS FORESHADOW SLOWDOWN IN TECH SPENDING

Cisco blamed political turmoil on the world stage for a slowdown in tech spending that will drive the company's overall revenue down in the current quarter.

The latest Cisco earnings report, released in November 2019, reflected a "pause" in spending by companies globally, Cisco CEO Chuck Robbins told financial analysts. The number of product orders in the quarter ended Oct. 26 fell in three customer segments – enterprise, commercial and service provider. Only the government sector showed positive growth.

"It feels like there's a bit of a pause [in spending]," Robbins said during the company's quarterly earnings call. The slowdown led to only a 2% increase in revenue, to $13.2 billion in the first quarter of the 2020 fiscal year. Revenue in the previous quarter rose 6% year over year. For the current quarter, Cisco said revenue would drop between 3% and 5%.

Tight control on expenses last quarter drove net income up 5%, to $3.6 billion. Cisco earnings per share rose 12%, to 84 cents.Several events globally were making tech buyers nervous enough to delay spending, Robbins said. They included anti-China protests in Hong Kong, the trade war between China and the United States, England's messy exit from the European Union, impeachment hearings in the U.S. Congress and political turmoil in Latin America.
"Business confidence just suffers when there's a lack of clarity," Robbins said.

As a result, a significant number of deals were smaller than expected, some fell through and others were delayed, he said. Cisco, considered a bellwether of tech spending, reported in August a global weakening in demand. But while spending fell in the service provider customer segment, the rest had positive growth.

Last quarter, Cisco continued to struggle in the Chinese and service provider markets. Revenue in China fell 31%, compared with a 26% drop in the quarter ended July 27, while service provider orders fell 13%.

Service provider spending has fallen for several quarters. However, Cisco has predicted that sales would pick up next year, when it expects carriers to start overhauling their networks to support plans for 5G business services.

Within Cisco, the decrease in service provider sales is reflected in lower enterprise routing revenue. Also, enterprises are spending less on data centre routing as they move their business software to public clouds.

"Cisco's product lines are strong," Patrick Moorhead, principal analyst at Moor Insights & Strategy, said. "But the company's core market, enterprise routing, isn't growing a lot."

Eventually, several industry trends will force businesses to increase spending, Robbins said. Companies will need new technology to take advantage of carriers' 5G wireless networks and the higher bandwidth of the new Wi-Fi 6 standard. The increase in data traffic from those next-generation technologies would, for example, drive sales of 400 Gigabit switches.

"Technology is so absolutely core to their fundamental strategies that it just seems to me that the time that they're going to be able to pause will be shorter than what you've seen in the past," Robbins said.

AMAZON DOORBELL CAMERA LETS HACKERS ACCESS HOUSEHOLD NETWORK

A vulnerability detected in Amazon doorbell cameras made it possible for hackers to gain access to the owner's household computer network.

The weakness in the Ring Video Doorbell Pro IoT device was discovered by researchers at Bitdefender in June of this year. Researchers found that the credentials of the local wireless network were being sent through an unsecured channel using plain HTTP during the doorbell's setup process. By exploiting the flaw, an attacker physically near the device could get hold of the doorbell owner's Wi-Fi password and use it to interact with all the devices in the owner's household network.

With the ability to communicate with devices such as security cameras and NAS storage devices, an attacker could access and steal private photos, videos, emails, and documents. It would also make it possible for an attacker to mount man-in-the-middle attacks.

According to Bitdefender chief security researcher Alexandru “Jay” Balan, the vulnerability could even have allowed a particularly determined hacker to gain physical access to a property. Balan told Infosecurity Magazine: "With access to a user's Wi-Fi password and, implicitly, access to the user's home network, there's a lot that can be done since devices are less secure on the inside.

"It's possible that someone could hack a local system that can output sounds (like a computer or a sound system) and make it say 'Alexa, open the front door'; however, this is admittedly a stretch."

The video doorbell is an immensely popular home security device, with almost 17,000 reviews and more than 1,000 answered questions on the Amazon.com website.

Bitdefender disclosed the vulnerability to Amazon on June 24. Amazon began implementing a fix on 5 September, and as of now, all Ring Doorbell Pro cameras have received a security update that fixes the issue. This isn't the first time Bitdefender has found flaws in a security device.

"We uncovered vulnerabilities in Guardzilla indoor security cameras last year that showed significantly bigger issues," said Balan.

"There's no escaping someone finding security flaws in your products, no matter who you are." Worryingly, more than half of vendors alerted to vulnerabilities in their products take no action to resolve them.

"We actually appreciate Ring's response. They deployed the patch quickly," said Balan.

MICROSOFT AND NOKIA COLLABORATE TO ACCELERATE DIGITAL TRANSFORMATION

Microsoft and Nokia announced a strategic collaboration to accelerate transformation and innovation across industries with cloud, Artificial Intelligence (AI), and Internet of Things (IoT).

By bringing together Microsoft cloud solutions and Nokia’s expertise in mission-critical networking, the companies are uniquely positioned to help enterprises and communications service providers (CSPs) transform their businesses. As Microsoft’s Azure, Azure IoT, Azure AI, and Machine Learning solutions combine with Nokia’s LTE/5G-ready private wireless solutions, IP, SD-WAN, and IoT connectivity offerings, the companies will drive industrial digitalisation and automation across enterprises and enable CSPs to offer new services to enterprise customers.

BT is the first global communications service provider to offer its enterprise customers a managed service that integrates Microsoft Azure cloud and Nokia SD-WAN solutions.

BT customers can access this through a customer automated delegated rights service, which enables BT to manage both the customer Azure vWAN and the unique Agile Connect SD-WAN, based on Nokia’s Nuage SD-WAN 2.0.

To be continued on page 18

Jason Zander, executive vice president, Microsoft Azure, said: "Bringing together Microsoft's expertise in intelligent cloud solutions and Nokia's strength in building business and mission-critical networks will unlock new connectivity and automation scenarios."

"We're excited about the opportunities this will create for our joint customers across industries."

"We are thrilled to unite Nokia's mission-critical networks with Microsoft's cloud solutions," said Kathrin Buvac, President of Nokia Enterprise and Chief Strategy Officer. "Together, we will accelerate the digital transformation journey towards Industry 4.0, driving economic growth and productivity for both enterprises and service providers."

The cloud and IoT have ushered in the fourth industrial revolution, or Industry 4.0, wherein enterprises are embracing data to automate and streamline processes across all aspects of their businesses. By joining forces, the two companies are bringing solutions to market that will simplify and accelerate this journey for enterprises, as well as enable CSPs to play a key role in helping their customers realise the potential of industrial digitalisation and automation while also optimising and better differentiating their own businesses.

Microsoft and Nokia are partnering to help accelerate digital transformation for enterprises by offering connectivity and Azure IoT solutions that unlock connected scenarios across multiple industries including digital factories, smart cities, warehouses, healthcare settings, and transportation hubs such as ports, airports and more.

The Nokia Digital Automation Cloud (Nokia DAC) 5G-ready industrial-grade private wireless broadband solution with on-premise Azure elements will enable a wide variety of secure industrial automation solutions that require more reliable connectivity, efficient coverage and better mobility than traditional Wi-Fi networks provide. For example, connected smart tools and machines on manufacturing floors that enable increased productivity, flexibility and safety for workers, or autonomous vehicles and robots in industrial environments that improve automation, efficiency and overall safety.

Nokia's Nuage SD-WAN 2.0 solution now enables service providers to offer integration with Microsoft Azure Virtual WAN for branch to cloud connectivity, with the companies planning to offer more options for branch internet connectivity in 2020. By automating branch and hybrid WAN connectivity, enterprises will have simplified, faster access to cloud applications such as Office 365, integrated security from branch-to-branch and branch-to-Azure and reduced risk of configuration errors causing security or connectivity issues.

Furthermore, the companies are integrating Nokia's Worldwide IoT Network Grid (WING) with Azure IoT Central to make the onboarding, deployment, management and servicing of IoT solutions seamless. This integration provides CSPs with the opportunity to offer their enterprises a single platform including vertical solutions to enable secure connected IoT services, such as asset tracking and machine monitoring on a national or global scale. Enterprises will be able to use Azure IoT Central and partner solutions for faster and easier enablement and implementation of their IoT applications together with Nokia's IoT connectivity solutions.

Microsoft and Nokia are collaborating to host Nokia's Analytics, Virtualization and Automation (AVA) cognitive services solutions on Azure. These AI solutions will enable CSPs to move out of private data centres and into the Azure cloud to realise cost savings and transform operations for 5G. Predictive Video Analytics is an example of a joint solution that will ensure optimal video experiences for CSP subscribers, improving reliability by up to 60 percent.

YESWEHACK LAUNCHES THE WORLD'S FIRST BUG BOUNTY EDUCATIONAL PLATFORM

YesWeHack, Europe's leading bug bounty company, announced the launch of YesWeHack EDU, the world's first bug bounty education platform dedicated to cybersecurity training.

Taking advantage of recognised expertise in Coordinated Vulnerability Disclosure (CVD), which gives security researchers a route to disclose a vulnerability impacting a specific system or application, as well as its unique ecosystem of customers and researchers, YesWeHack EDU trains users to detect security vulnerabilities in realistic scenarios, identical to what exists today within organisations and governments.

"Cybersecurity has become an economic and societal issue. Disturbingly, the sector suffers from an imbalance

To be continued on page 19

between the state of the threat and the market's actual defence capabilities," commented Kevin Gallerin, Managing Director, Asia Pacific, YesWeHack. "To remedy this, the capacity of public and private actors to detect and correct shortcomings in a professional and ethical manner must be rapidly strengthened — and this requires specialised training and better information sharing."

Aimed at Information Technology and specifically, cybersecurity curriculums in schools and universities, YesWeHack EDU's educational approach encourages simulation through gamification and the involvement of each student in securing their institution. Above all, it opens up prospects for future developers towards promising specialisations such as DevSecOps, Data Scientist, Security Analyst, and related job titles. Finally, YesWeHack EDU facilitates the implementation of collaborative projects and cross-functional initiatives between academic institutions and the private sector.

The launch of the EDU platform comes on the back of several other initiatives with the education sector, including a recent bug-bounty workshop organised in partnership with Singapore Polytechnic.

"According to a study published by Gartner, 50% of companies worldwide are expected to implement bug bounty programmes by 2022, compared to just 5% today. We are launching YesWeHack EDU to address the severe talent shortage currently facing the cybersecurity industry. This program will also provide the academic community with a sophisticated training platform that will professionalise vulnerability management and provide further training for the new age of cybersecurity roles," explains Kevin Gallerin, Managing Director, Asia Pacific, YesWeHack.

Available globally, the YesWeHack EDU platform is aligned with the SPARTA consortium initiative, of which YesWeHack is a founding member, that aims to strengthen both innovation and research in cybersecurity at the European level.

CYBERSECURITY SKILLS SHORTAGE TOPS FOUR MILLION

Global IT security skills shortages have now surpassed four million, according to (ISC)2.

The certifications organisation compiled its latest Cybersecurity Workforce Study from interviews with over 3200 security professionals around the world.

The number of unfilled positions now stands at 4.07 million professionals, up from 2.93 million this time last year. This includes 561,000 in North America and a staggering 2.6 million shortfall in APAC.

The shortage of skilled workers in the industry in Europe has soared by more than 100% over the same period, from 142,000 to 291,000.

The report estimated the current global workforce at 2.93 million, including 289,000 in the UK and 805,000 in the US.

Nearly two-thirds (65%) of responding organisations reported a shortage of cybersecurity staff, with a lack of skilled or experienced security personnel their number one workplace concern (36%).

(ISC)2 claimed the global security workforce needs to increase by a staggering 145% to cope with a surge in hiring demand. In Europe, this has come particularly in smaller companies with one-99 employees, as well as those with over 500 employees.

Unsurprisingly, over half (51%) of cybersecurity professionals said their organisation is at moderate or extreme risk due to staff shortages.

The report pointed to four key strategies to help organisations tackle such shortages. These include in-house training and development and setting applicant qualification requirements at the right level to ensure as wide a net as possible is cast.

(ISC)2 also stressed the need to attract new workers from other professions, or recent graduates with tangential degrees, as well as seasoned professionals from consulting and contracting sectors. Finally, organisations should look to strengthen from within by cross-training existing IT professionals where appropriate.

AUSTRALIAN GOVERNMENT PROPOSES NATIONAL CYBER REGIME FOR IoT

Everyday Internet of Things devices such as AI-enabled smart speakers and smart TVs will be subject to a new Australian code of practice to better protect against malicious cyber threats.

With concerns over the always-on devices and privacy reaching fever-pitch, the federal government has moved to introduce voluntary national standards for IoT security.

The code, developed by the Department of Home Affairs and Australian Cyber Security Centre, will offer best practice guidance to device manufacturers, IoT service providers, and app developers.

Minister for Home Affairs Peter Dutton said that ensuring the security of everyday smart devices, which Gartner estimates will reach more than 64 billion globally by 2025, was "paramount".

He said that currently "many of these devices have poor cybersecurity features", which poses risk to Australians, the economy and national security.

The draft code, which the government is currently seeking community and industry input on, lays down the 13 cybersecurity principles that industry will be expected to embed in IoT devices.

"Devices are often developed with functionality as a priority, with security being absent or an afterthought," the draft code states.

"It is essential that these devices have cyber security provisions to defend against potential threats."

While the government recommends implementing all 13 principles, the first three are considered the "highest priority to achieve the greatest security benefit". These principles are:

No duplicated default or weak passwords: ensure IoT device passwords aren't weak or a factory default common to multiple devices

Implement a vulnerability disclosure policy: ensure there is a public point of contract for security researchers to report issues and that that any vulnerabilities are acted on quickly

Keep software securely updated: ensure "timely" updates, which are distributed via secure IT infrastructure, that don't change user-configured preferences, security or privacy

Other principles include ensuring credentials aren't stored on a device to avoid that data being discovered through reverse engineering (principle 4), minimising the exposed attack surface (principle 6) and making systems resilient to outages (principle 9).

The government has also recommended "adequate industry-standard encryption...be applied to personal data in transit and data at rest" in order to ensure that personal data is protected (principle 5).

"We're releasing the Code of Practice for public consultation because we want to ensure that the expectations of all Australians are met regarding cyber security," Dutton said.

"Along with our Five Eyes partners we share the expectation that manufacturers should develop connected devices with security built in by design."

The code aligns with and builds upon similar guidance issued by the UK in its code of practice of consumer IoT security [pdf], which also consists of 13 principles.

RETARUS MOVES UP THE QUADRANT IN RADICATI'S SECURE EMAIL GATEWAY 2019 REPORT

In its recent analysis of the Secure Email Gateway market, Radicati Group rated information logistics expert Retarus the 'Trail Blazer' with the very best positioning, attributing to its innovation in the Email Security Services portfolio. The only privately managed European organisation to land a spot in this competitive report, Retarus has progressed towards the 'Top Player' segment from its previous assessment at the beginning of the year. Service providers ranked in this category distinguish themselves mainly through offering innovative technologies and their ability to shape the product landscape.

The report emphasises how Retarus facilitates enterprise organisations with multi-facetted range of services to fulfil their mission-critical business requirements. Additionally, Radicati highlights Retarus' progressive portfolio of Email Security Services and the benefits it offers including Email Continuity, making it the only privately-managed European organisation to land a spot in this quadrant.

In Radicati's analysis, the Email Continuity Services recently launched by Retarus add a significant value for companies looking to implement a comprehensive cybersecurity strategy. Since email is the most essential communication channel for enterprises, followed by telephone and fax, it is crucial to avoid outages by all means.

Retarus' Email Continuity Services enable this seamless flow of communication, even in the event of customer's email system failures caused by cloud downtimes or data centre outages. The service allows the impacted organisations to switch

To be continued on page 21

over flexibly and conveniently, to a platform running concurrently in the background at all times. In addition, Retarus' Email Continuity Services fulfil all key criteria to enable a successful disaster protection.

Eradicating the need for companies to spend a lot of time and effort starting up their own back-up email systems, Retarus allows the services to run independently of the technology utilised by the company, for instance Microsoft Exchange. Retarus offers this feature to companies of all sizes, and 120,000 users from an organisation recently benefited from connecting to the system as part of a pilot program.

With its patented Postdelivery Protection service Patient Zero Detection(R), according to Radicati, Retarus E-Mail Security has achieved an additional security dimension, which successfully protects users from being harmed by malware in emails that have already been delivered to their inboxes. Patient Zero Detection(R) Real-Time Response processes threats and enables emails infected with malware that have been detected within the company's infrastructure to be deleted automatically or moved to a special folder for further analysis.

The experts at Radicati also draw attention to the web-based Enterprise Administration Services portal, which provides Retarus' customers with an opportunity to configure their own services more efficiently. Furthermore, Retarus offers a real-time search option 'Email Live Search' including analysis and IT forensics functions, which the analysts describe as efficient and easy to use. Within the scope of this service, for instance, Retarus makes forensic data available in real time for the customer's SIEM processes (Security Information and Event Management).

Additional features offered by Retarus Email Security Services, such as Advanced Threat Protection (ATP) with Sandboxing, Deferred Delivery Scan, Time-of-Click Protection (URL-Rewriting) and CxO Fraud Protection (Anti-Spoofing and Anti-Spear-Phishing) as well as flexible access management and encryption, have already received recognition by Radicati in their previous report.

"Our positioning in the top right corner of Radicati's 'Trail Blazer' quadrant, near to the 'Top-Player' segment, is a clear affirmation of our email security strategy," says Martin Hager, founder and CEO at Retarus. "Retarus is the only European and owner-led company with a multi-dimensional approach for corporations and huge, multinational companies providing users with optimum protection from email threats - in combination with compliance features, user-friendliness and sensible integration into eco-systems. This excellent positioning will spur us on to continue augmenting our services with additional functions that provide companies with real added value."

TREND MICRO EMPLOYEE SELLS CUSTOMER DATA

An employee of trusted cybersecurity firm Trend Micro has been fired after illegally accessing and selling customer data to a malicious third party. An estimated 68,000 English-speaking customers were affected by the insider threat incident, which was disclosed by Trend Micro at the start of November 2019.

Trend Micro's suspicions were first aroused in early August 2019, when customers running the company's home security solution began reporting that they had received calls from scammers purporting to be Trend Micro support personnel.

In a statement shared on the company website, a Trend Micro spokesperson wrote: "The information that the criminals reportedly possessed in these scam calls led us to suspect a coordinated attack."

An investigation was "immediately launched" by Trend Micro, but it wasn't until October 2019 that the company was able to say for sure that the scam phone calls had stemmed from an insider threat.

Information that ended up in the hands of the criminal scammers included names, email addresses, and telephone numbers. The identity of the malicious third party who bought the information from the rogue Trend Micro employee, and how much they paid for the stolen data, is currently unknown.

A Trend Micro spokesperson wrote: "A Trend Micro employee used fraudulent means to gain access to a customer support database that contained names, email addresses, Trend Micro support ticket numbers, and in some instances telephone numbers.

"There are no indications that any other information such as financial or credit payment information was involved, or that any data from our business or government customers was improperly accessed."

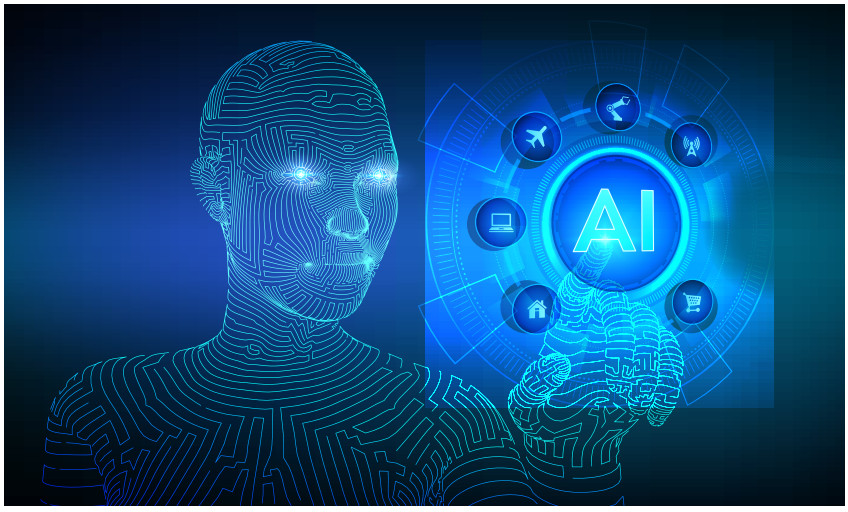
Upon discovering the wounding betrayal by one of their own, Trend Micro immediately disabled the unauthorised account access and fired the insider threat culprit. The incident is currently under investigation by law enforcement.

In a statement released on their website, Trend Micro reminded their customers that the company never makes unsolicited phone calls to consumers.

A company spokesperson wrote: "If a support call is to be made, it will be scheduled in advance. If you receive an unexpected phone call claiming to be from Trend Micro, hang up and report the incident to Trend Micro support."

IBM IoT LAUNCHES AI-POWERED MONITORING SOLUTION WITH ANOMALY DETECTION

IBM announced Maximo Asset Monitor, a new AI-powered monitoring solution designed to help maintenance and operations leaders better understand and improve the performance of their high-value physical assets.



An extension of IBM's market-leading IBM Maximo capabilities, this new solution will help unlock essential insights with AI-powered anomaly detection and provide enterprise-wide visibility into critical equipment performance. The result is faster problem identification that can inform better decisions and reduce downtime.

According to a 2016 report by analyst firm Aberdeen Research, unplanned downtime can cost a company as much as $260,000 an hour. A comprehensive view of asset performance across operations may help reduce downtime, but that visibility has been difficult to achieve due to fragmented legacy systems, data silos and geographic barriers. With Maximo Asset Monitor, organisations can now aggregate data from across the enterprise and combine it with advanced predictive analytics and AI to identify operational patterns.

Capabilities like AI-powered anomaly detection can help organisations identify the most important alerts among the hundreds generated daily from critical assets. This can help teams respond quickly to the most critical anomalies and gain greater insights into root cause variables that lead to asset failure.

Kareem Yusuf, Ph.D., general manager, IBM IoT, said: "As critical assets become more connected, intelligent and complex, the model for operating and maintaining them must evolve. Organisations must move faster to spot patterns and react to maintenance issues quickly, accurately and safely."

"With the launch of the new Maximo Asset Monitor solution, IBM is helping organisations better understand their data and automate workflows with preventative, predictive, and prescriptive maintenance actions to help extend asset life and improve operations. According to IDC, monitoring performance and scheduling repairs with predictive maintenance can reduce maintenance costs by 15-20%, improve asset availability by 20%, and extend the lives of machines by years."

IBM is recognised by analyst firm IDC as a leader in Enterprise Asset Management applications. IBM Maximo is deployed across 99 countries, seven continents, and isused by many of the world's largest organisations. IBM has a long history of working with organisations like Novate Solutions®, Inc. to help monitor and manage their assets and operational performance.

Novate Solutions is an industrial technology and engineering services firm in California that is collaborating with IBM to develop a new, scalable, remote monitoring and support service for industrial manufacturers. The application of IBM Maximo Asset Monitor enabled by AI and analytics leverages existing infrastructure collected from SCADA systems to detect anomalies to predict system failures.

The analysis of data by engineering professionals at Novate's Support Operations Centre provides insights into the root cause of an anomaly and its process implications. These experts are able to identify events that may warrant immediate proactive intervention which enables maintenance and engineering support teams to take action before the control system is designed to react. The ultimate goal of Novate is to improve production reliability and reduce costly unplanned downtime.

"Our goal is to revolutionise how industrial manufacturers utilise data and technology to improve production metrics by providing a scalable service that virtually every manufacturer can afford. We are collaborating with IBM to enable this transformation by leveraging AI technology with IoT data and analytics," said Rob Mora, executive vice president, Novate Solutions®, Inc.

"The ability to recognise anomalies in real-time and proactively make changes to operations can have a tremendous impact on increasing plant reliability and driving continuous improvement for manufacturers of any size."

DRONE WARS: EXPERTS WARN OF FLYING NETWORK SECURITY THREAT

Drones could become a major network security threat from 2020, forcing organisations to guard the airspace around their buildings, security researchers have warned. Small unmanned aerial vehicles (UAVs) will increasingly evolve from novelty items to "ubiquitous business tools" over the coming years, explained defence contractor Booz Allen Hamilton in a new 2020 Cyber Threat Trends Outlook report.

However, as they do, cyber-criminals may also look to take advantage by flying them close to target networks and/or landing them in concealed locations such as on roofs. In this way, a UAV could be fitted with a Wi-Fi Pineapple and used as a rogue access point to harvest credentials, perform man-in-the-middle attacks against employees and carry out network reconnaissance, the report warned. IoT devices such as smart light bulbs, or even wireless mice could also be targeted.

"Drones equipped with specially fitted hardware and software may also be used to install malicious malware on systems or disrupt system's operations, particularly devices that are vulnerable to exploitation of wireless protocols like Bluetooth and ZigBee," the report claimed.

"The requirement for both the attacker and the drone to be in proximity to a target (e.g., Bluetooth has an estimated maximum range of 300 feet) will limit the frequency with which drone-based attacks will be used, but the threat nonetheless remains real."

To mitigate the threat, Booz Allen Hamilton urged organisations to consider training physical security staff to spot drones, installing jamming signals and treating their airspace as an extension of the corporate attack surface.

"For small / home office wireless networks, operators may consider mitigations commonly used to address war-driving attacks, such as turning off the wireless network when not in use, updating administrator passwords on routers regularly, and using security measures such as wireless traffic encryption and firewalls," it added.

Elsewhere in its report, the IT consulting giant warned of a growing risk to satellite infrastructure, connected cars, the upcoming Tokyo Olympics, and digital elections.

KAPE TECHNOLOGIES BUYS ONLINE PRIVACY COMPANY LTMI FOR $128 MILLION

London-listed Kape Technologies PLC announced the acquisition of Colorado-based LTMI Holdings, whose main asset is online privacy company Private Internet Access (PIA), for $127.6 million. Kape will pay $95.5 million in a cash and stock deal, and also pay off LTMI's debt of $32.1 million. Kape will fund the deal using its free cash flow and a $40 million shareholder loan extended by its controlling shareholder, Israeli businessman Teddy Sagi. Sagi holds a 73% stake in the company, which he acquired in 2013 for $37 million. Following the merger, his stake will be reduced to 55.9%

PIA, which specialises in digital encryption and virtual private networks (VPN), employs 65 people, a third of them in research and development. The rest of LTMI's assets also pertain to online privacy. Kape has stated the acquisition will enable it to cement itself as a leading player in the privacy sector.

Following the acquisition, Kape expects to double its number of paying clients to over two million. According to the announcement, half of LTMI's million-plus subscribers are in the U.S., which will make Kape the largest player in the sector in the country following the acquisition. The company forecasts revenues of between $120 million and $123 million for 2020 for the merged entity, and an EBITDA of between $35 million and $38 million. LTMI's revenues for 2018 stood at $47.4 million, an 18% increase year-over-year, and its adjusted EBITDA was $14.7 million. Kape also said it expects annual cost savings of up to $4.5 million following infrastructure reductions.

Kape, founded in 2011, is a cybersecurity company developing online security, privacy, and autonomy products. Kape operates in 160 countries and employs 300 people, 70 of them in its Israeli research and development centre. The company listed on the London Stock Exchange's AIM market in 2014 and currently has a market capitalisation of $142 million.

Kape reported revenues of $29.9 million for the first half of 2019, a 24.2% increase year-over-year, and an EBITDA of $5.8 million, up from $4.7 million in the first half of 2018. The company has $36.4 million in its coffers as of the end of June 2019.

This is Kape's largest acquisition to date and the fourth since CEO Ido Erlichman assumed his position in May 2016. In 2018, Kape acquired cybersecurity company Netural Holdings Ltd., trading as Intego, for $16 million, and VPN provider ZenMate for $5.6 million. In 2017, the company paid $10.3 million for VPN provider CyberGhost SA.

Following the acquisition, LTMI CEO Ted Kim will join Kape's board of directors and take over the merged company's North American operations.

ICO SAYS UK POLICE MUST 'SLOW DOWN' USE OF FACIAL RECOGNITION TECHNOLOGY

The Information Commissioner's Office (ICO) is calling on police forces to slow down and properly justify their use of live facial recognition (LFR) technology.

Following a 17-month investigation into UK police forces' use of LFR, the ICO is recommending that the government introduce a statutory and binding code of practice on its deployment.

The findings and recommendations have been collected in a report of the investigation, which said: "The absence of a statutory code of practice and national guidelines contributes to inconsistent practice, increases the risk of compliance failures, and undermines confidence in the use of the technology."

In a blog post, information commissioner Elizabeth Denham said the report's recommendations had such far-reaching implications for law enforcement's use of the technology that she felt it necessary to publish a Commissioner's opinion. The opinion aims to guide police and other law enforcement bodies, such as the Home Office, on how to deploy LFR, and is the first of its kind to be issued under data protection legislation introduced in 2018.

In the opinion, Denham said the use of LFR in a law enforcement context constituted sensitive processing because "it involves the processing of biometric data for the purpose of uniquely identifying an individual".

She added: "Controllers must identify a lawful basis for the use of LFR. The commissioner expects that to give the public confidence in police use of LFR, more detail is required in data protection impact assessments [DPIAs]."

In Denham's view, the legislative requirement that this type of data processing should be "strictly necessary" has not been properly addressed in previous DPIAs.

In the case of South Wales Police, one of the forces spearheading the use of LFR, its DPIA considers the processing of biometric data using LFR to be strictly necessary, as "it would be almost impossible for any one officer to be able to effectively remember and identify several hundred individuals from their face alone". ANALYSIS computerweekly.com 19-25 November 2019 5 Home News ICO says UK police must 'slow down' use of facial recognition technology How Microsoft is applying AI to Lego building and software security How the CIO at Northampton General Hospital NHS Trust is consigning paper records to the past Editor's comment Buyer's guide to next-generation programming tools Addressing UK's skills gap in the face of Brexit DevOps and storage: APIs and flexibility key Downtime.

Similarly, although the Metropolitan Police Service's DPIA points out that the processing must be "strictly necessary", it does not explain how the force is meeting this requirement.

The commissioner's opinion also considered the High Court's recent ruling that South Wales Police's use of LFR was lawful as it had "struck a fair balance and was not disproportionate".

Although generally supportive of the ruling, the ICO took the view that the combination of law and practice that were relied on by South Wales Police could be made "more clear, precise and foreseeable so that individuals can better understand when their biometric data may be processed by LFR".

Denham warned that the High Court's decision should not "be seen as a blanket authorisation to use LFR in all circumstances".

RANSOMWARE ATTACK ON CANADIAN TERRITORY

Nunavut, Canada's largest and most northerly territory, was struck by a ransomware attack at the start of November 2019.

The sophisticated cyber-assault was launched on the sparsely populated territory's government network at approximately 4:00 am on 2 November 2019, resulting in the swift encryption of multiple Word documents and PDF files.

Users trying to access the infected government network were confronted with a ransom note that read: "Your network has been penetrated. All files have been encrypted with a strong algorithm...we exclusively have decryption software for your situation." The threat actors behind the attack instructed users to download an encrypted browser and visit a specific URL within the next 21 days. Users were told that the sooner they pay, the lower the price they will be charged to recover their encrypted files.

To be continued on page 25

In an attempt to contain the attack, the government shut down parts of its network, leaving many government employees unable to access their email or voicemail. All government services requiring access to electronic information were impacted by the attack, with the exception of Qulliq Energy Corporation.

"The nature of the government is we're a centralised organisation, so it has impacted the file servers of different departments and it's impacted some of our communities as well," Nunavut's director of information, communications, and technology, Martin Joy, told CBC News.

The ransomware is believed to have been triggered when an employee working late on Friday night clicked a link in a malicious email or web advertisement. Joy said the ransomware appeared to be DoppelPaymer, which Nunavut's security systems hadn't been trained to detect.

In a statement released, the Nunavut government wrote that "there is no concern at this time with the loss of personal information or privacy breaches."

Contingency plans have been implemented to ensure uninterrupted services to the local community, and the government stated that it "expects the majority of files will be restored, using existing up-to-date back-ups." Minister of Community and Government Services Lorne Kusugak said in a statement in the legislature that it would be at least a week before services were restored.

Speculating on why threat actors might have targeted Nunavut, Emsisoft's Brett Callow commented: "US entities are on very high alert, bolstering their IT, and so are less likely to be compromised. Because of this, big game hunters are increasingly looking for opportunities in other countries."

AVTECH SWEDEN'S PROFLIGHT HELPS PILOTS PICK THE PERFECT FLIGHT PATH

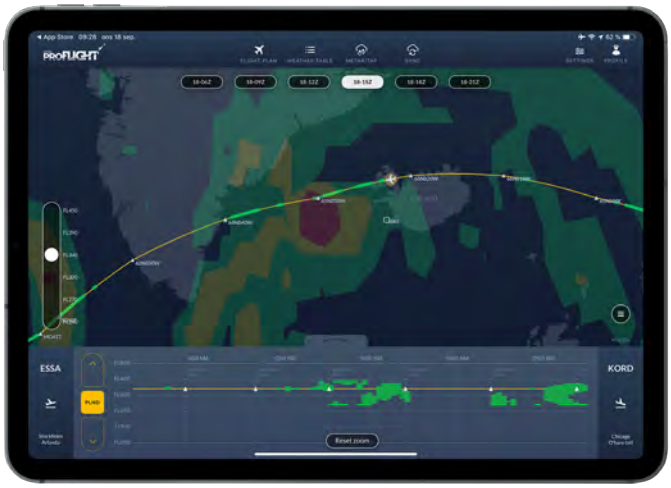
Thunderstorms are not usually dangerous for airplanes, but they are often followed by turbulence that really can rock. Now all airline pilots have an option to try out an easy-to-use app, proFLIGHT by Swedish AVTECH, that very precisely shows where the actual threats are in real time along the trajectory.

There is no witchcraft behind the app, but very accurate 10K weather data from Met Office UK, in combination with IATA's Turbulence Aware observations (for participating airlines) as well as real-time satellite thunderstorm data, provided by Airbus Defence and Space GmbH.

"All this information is continuously updated in our back-end systems and available to proFLIGHT users at all time", says Niklaes Persson, Head of R&D at AVTECH and a commercial airline pilot himself. "To put it shortly, our back-end system takes in enormous amounts of weather-related data all the time, which is then refined on-demand to single trajectories that can be sent to the aircrafts through normal aviation communication channels."

Persson explains that thunderstorms are usually caused by Cumulonimbus, abbreviated CB, which is a vertical cloud that is capable of producing lightning and other dangerous severe weather when carried upward by powerful air currents.

"Now the app includes a new CB layer that displays current position and the state of CB-cells on a single aircraft's route", he says. "In addition, proFLIGHT now also includes a



forecast of the development and movement for each of the cells with an accuracy of about one hour. This way the pilot can choose the best route to avoid probable turbulence."

The CB layer in proFLIGHT is based on real-time satellite observations of CB-clouds.

"Their first intention was to provide data from only a smaller part of Europe, since the satellite data is very expensive", Persson says. "When the project evolved, however, Airbus opened up a corridor for us all the way to Asia. So now we can offer a truly outstanding possibility for aircrafts to avoid thunderstorms and turbulence along their trajectories on many of the major routes from Europe to Asia."

MALWAREBYTES REPORTS A 60 PERCENT JUMP IN HEALTHCARE ENDPOINT THREAT DETECTIONS

Malwarebytes, the leading advanced endpoint protection and remediation solution, announced the results of its latest Cybercrime Tactics and Techniques (CTNT) report, "CTNT Q3 2019: The State of Healthcare Cybersecurity." Malwarebytes observed a 60 percent increase in threat detections at healthcare organisations by comparing all of 2018 against just the first three quarters of 2019, demonstrating significant growth and reason for increased concern about healthcare security as we move into 2020.

According to Malwarebytes' product telemetry, the healthcare industry has been overwhelmingly targeted by Trojan malware during the last year, which increased by 82 percent in Q3 2019 over the previous quarter. The two most dangerous Trojans of 2018–2019 for all industries, Emotet and TrickBot, were the two primary culprits. Emotet detections surged at the beginning of 2019, followed by a wave of TrickBot detections in the second half of the year, becoming the number one threat to healthcare today. Due to aging infrastructure, low IT budgets and a wealth of personally identifiable information (PII), healthcare institutions are becoming prime targets for cybercriminals.

"Healthcare is vital to our population, industries, and economy, which is why it's an especially concerning industry to see targeted by cybercriminals," said Adam Kujawa, Director of Malwarebytes Labs. "Emotet, TrickBot, exploit, and backdoor detections targeting healthcare organisations are known to drop ransomware payloads later in their attack chains. For too long, these organisations have suffered due to antiquated equipment and underfunded IT departments, making them especially vulnerable. We should be arming healthcare now with extensive security measures because this pattern suggests that ransomware is looking to penetrate healthcare organisations from several different angles."

"With the Health Ministry in Singapore setting aside $6.1 billion to support healthcare subsidies and schemes alone, more expenditure is expected to be pumped into boosting healthcare services and technology. It is imperative that new innovations and technologies are introduced alongside adequate security measures, with proper staff training and incident response protocols set in place to ensure utmost vigilance against cyber breaches. The public can also play their part in keeping themselves informed about potential threats, to avoid falling victim to scams that seek to exploit personal data from them." expressed Jeff Hurmuses, Area Vice President and Managing Director, Asia Pacific, Malwarebytes.

REGULATION ASIA HONOURS AXIOMSL WITH TWO AWARDS

AxiomSL received two Regulation Asia Awards for Excellence 2019 at a ceremony in Singapore on 13 November 2019, winning the coveted Best Solution in Regulatory Reporting award and the Regtech Award for Cloud Innovation.

"We are proud to have been presented with two awards this year," said Peter Tierney, AxiomSL's APAC General Manager. "Not only are we delighted to be singled out as best in class for our data integrity and control platform and risk and regulatory solutions, but we are thrilled that Regulation Asia recognises the value of RegCloud™, our innovative cloud deployment offering. Clients across the Asia Pacific region are already benefiting from the efficiencies and economies of scale gained by deploying AxiomSL's platform and solutions—including MAS 610, HKMA, APRA-EFS, and Global Shareholding Disclosures—on its well-architected, highly secure RegCloud," added Tierney.

Financial institutions benefit from AxiomSL's innovative, transparent regulatory compliance and reporting ecosystem that efficiently satisfies a broad range of regulatory requirements, quickly incorporates regulatory changes, provides dynamic data-lineage that supports audit defence, and enables business-critical insights into risk management. "In today's Basel-driven environment, firms increasingly leverage ControllerView's deep capabilities to run their risk management and Basel compliance programs," commented Tierney.

"The Basel Committee on Banking Supervision's (BCBS) standard 239 sets the parameters for enterprise risk management (ERM), a foundation upon which business units, governance, and risk functions can mutually evolve," said Abraham Teo, Head of Products, APAC for AxiomSL. "To this end, AxiomSL's data integrity and control platform—the antithesis of a black box—delivers transparent risk capital and return calculations with reporting choices that satisfy regulatory requirements," Teo added. "With its ability to seamlessly ingest disparate data and its end-to-end automation processes, ControllerView provides clients

To be continued on page 27

with the clarity and information they need to build higher-quality capital and liquidity reserves, thus increasing their capacity to buffer unexpected losses and weather liquidity crises," continued Teo.

"Innovation is at the heart of AxiomSL's core technology," said AxiomSL's Eric Rothrock, Senior Vice President, Cloud Product Management. "We are proud to continue that innovation journey with RegCloud, our highly secure, fully managed, cost optimised RegCloud."

AxiomSL deploys RegCloud based on a secure, single-tenant virtual private cloud (VPC) for each client. "Security is paramount as financial institutions consider going to the cloud. This year, we achieved ISO 27001 certification and SOC 2 Type II attestation as part of a comprehensive approach to ensuring the security of sensitive material non-public information (MNPI) on RegCloud," commented Rothrock. Clients utilising RegCloud experience key outcomes including optimised application reliability and performance, continuous alignment with regulatory requirements, efficient delegation of security and maintenance, quicker time-to-value, and ongoing cost savings. Relieved of the burden of owning and operating complex hardware and software infrastructures, firms utilising RegCloud discover that they can focus on their core business and become more agile and innovative.

"Receiving Regulation Asia's award for Cloud Innovation is an exciting validation that financial institutions in Asia Pacific and globally are ready to consider the cloud for their risk and regulatory data and reporting —when the implementation meets their expectations for security and efficiency, as does RegCloud," Peter Tierney concluded.

INGRAM MICRO NAMED CHECK POINT SOFTWARE TECHNOLOGIES DISTRIBUTOR FOR SINGAPORE

Ingram Micro announced a new relationship with Check Point Software Technologies (Check Point) to drive the adoption of Check Point solutions in Singapore and Malaysia. Check Point is the world's leading cyber security provider, offering the most comprehensive and cutting-edge cyber security technology across network, data, endpoints, cloud, and mobile.

Ingram Micro delivers a full spectrum of global technology and supply chain services to businesses around the world. Deep expertise in technology solutions, mobility, cloud, and supply chain solutions enables its business partners to operate efficiently and successfully in the markets they serve. Unrivalled agility, deep market insights and the trust and dependability that come from decades of proven relationships, set Ingram Micro apart and ahead. Ingram Micro operates in 160 countries, including Singapore, Thailand, Hong Kong, Malaysia, and Indonesia.

Through its complete security architecture, Infinity, Check Point defends an organisation's IT elements, from networks and end point devices to cloud based applications and infrastructure to mobile devices. This comprehensive security is served while equipping customers with an effective and intuitive security management addressed to thwart and prevent the ever-changing landscape of cyber threats. Check Point addresses 5th-generation cyber-attacks or "Gen-V" attacks, which are large-scale and fast-moving attacks that easily bypass the conventional, static detection-based defences used by most organisations today.

Evan Dumas, Regional Director, Southeast Asia, Check Point Software Technologies, said, "We are pleased to appoint Ingram Micro as a Check Point distributor in Singapore and Malaysia. Our new relationship with Ingram Micro will enable us to reach out to various market segments and provide organisations of all sizes with innovative and effective security solutions that keep them protected even against the most advanced threats."

Francis Choo, vice president and Chief Country Executive, ASEAN & HK, Ingram Micro said, "We are excited to enhance our security offering to our partners with the additional of Check Point to our portfolio. The rise in hybrid data centre adoption and the exponential growth in mobile devices increase the importance for businesses to look into their security set-up and coverage. The combination of Check Point's solutions and our aggregated security services and solutions - spanning consulting to delivery – will meet the needs and opportunities in the market."

JAPAN'S LINE LAUNCHES PUBLIC BUG BOUNTY PROGRAM WITH HACKERONE

HackerOne, the number one hacker-powered pen-test and bug bounty platform today announced the launch of LINE Corporation's ("LINE") public bug bounty programme. Through the programme, ethical hackers are invited to test LINE's core messenger application and web domains for potential vulnerabilities and securely disclose them to LINE. In working with HackerOne, LINE is able to tap into the vast expertise of a global community of skilled hackers to identify and fix security vulnerabilities before they can be exploited.

Since July 2019, LINE has been running a private program on HackerOne in tandem with its self-managed bug bounty program. Over the course of the past four months, LINE has paid out nearly US$30,000 in monetary awards — better known as bounties — to hackers for their efforts and has seen increased engagement from hackers internationally. In going public, the company will be transitioning its entire bug bounty ecosystem to the HackerOne platform. Since starting its ongoing bug bounty program in June 2016, the company has received more than 1,000 reports and has paid over US$300,000 in bounties through both self-run and HackerOne bug bounty initiatives.

"We are thrilled to be moving to the HackerOne platform as it allows us to increase our visibility and thereby increase the amount of high quality reports we receive as well," said Naohisa Ichihara, Head of Cyber Security Department at LINE. "As being transparent about security issues is very important to us, we wanted a convenient way to disclose such information. Our original platform did not have an easy way of achieving this, so it was also a contributing factor in deciding to move to HackerOne."

There are over 570,000 hackers registered on HackerOne. Participation in the LINE bug bounty program is open and encouraged to all hackers worldwide. Bounty awards range from US$500 to US$30,000 for eligible valid vulnerabilities.

Assets in scope include the main LINE application (for iOS, Android, Chrome, MacOS and Windows) as well as the web domains https://store.line.me/, https://news.line.me/, https://music.line.me/, and https://live.line.me/.

"With 164 million global monthly average users across their top four countries, LINE knows it's imperative to protect user information around the clock," said Attley Ng, HackerOne's VP, Asia Pacific (APAC). "By adding the largest community of ethical hackers in the world as an extension of their cybersecurity team, LINE enhances their global approach to security and improve the safety of their customers."

APAC continues to be one of the fastest growing regions for hacker-powered security. According to HackerOne's 2019 Hacker Powered Security Report, the number of hacker-powered security programs grew by 30% in the region year over year. This new program comes on the heels of a momentous year of growth in the region for HackerOne. The company opened its APAC headquarters in Singapore and has brought on notable customers including Ministry of Defence Singapore (MINDEF), GovTech Singapore, Xiaomi, Zomato, Toyota, Nintendo, Grab, and Alibaba. In addition, the region's first ever live-hacking event (h1-65) was held in Singapore, with Dropbox awarding over $300,000 in bug bounties to participating hackers.

NTT LTD. HONOURED WITH TWO GLOBAL AWARDS AT CISCO PARTNER SUMMIT 2019

NTT Ltd., a world-leading global technology services provider, today announced that it has received two Cisco® Partner Summit Global awards, recognised as APJC Partner of the Year and Software Partner of the Year. Cisco announced the winners at a Global Awards reception during its annual partner conference that took place this week in Las Vegas, Nevada.
It was also revealed that Asia Pacific received regional awards in the following categories – Architectural Excellence: Security, Cisco Capital Partner of the Year, Learning Partner of the Year, as well as Partner of the Year for Greater China and India.

Awarded to channel partners who rise to business challenges, the Cisco Partner Summit Global awards

To be continued on page 29

are designed to recognise superior business practices and reward best-in-class methodologies. Areas of consideration include innovative processes, architecture-led successes, strategic business outcome-focused programs, seizing new opportunities, and sales approaches.

"It gives me great pleasure to recognise these partners who continue to demonstrate superior performance and drive value for our customers. They demonstrate superior leadership and innovation to help enterprises solve complex problems," said Oliver Tuszik, senior vice president, Global Partner Organisation, Cisco. "It's an honour to present the APJC Partner of the Year and Software Partner of the Year awards to NTT Ltd. in recognition of its outstanding achievement in helping customers respond to their business challenges."

Jan Wuppermann, Senior Vice President, Asia Pacific – Strategy & Business Operations at NTT Ltd. said, "I'm extremely proud of our joint achievements and successes. We look forward to continuing our partnership with Cisco to deliver value to our clients around the world."

Doc Watson, Group Executive – Global Cisco Alliance at NTT Ltd. said, "We are proud to once again be recognised by Cisco with a double award win this year. For 28 years now, we have been working in partnership with Cisco to co-innovate together. We share and leverage our intellectual property, including products and code, which allows us to move faster with a focus on applied innovation to challenge the art of the possible. This will ultimately result in some exciting innovations for our clients. Our joint initiative Connected Conservation protecting rhinos in South Africa is a great example of how, together, we're making a huge difference in the real world. Our joint technology ventures have the power to change lives both at a global and country level and these awards are a testament to that."

TOSHIBA TO FORM IOT ALLIANCE WITH SOFTBANK, KDDI AND OTHERS

Japanese electronics conglomerate Toshiba will launch an "internet of things" platform that will include companies like SoftBank Group, wireless carrier KDDI and utility Tokyo Gas.

Toshiba will create an association of roughly 100 Japanese companies called ifLink Open Community, the company announced on Tuesday. The group will be established by the end of March. The global internet of things market totalled $646 billion last year, according to U.S. researcher IDC, and is forecast to surpass $1 trillion in 2022.

It is a significant step for Japanese companies that are struggling to break into the growing technology sector. More than 90% of Japanese businesses say they lack information technology specialists, according to a recent government white paper. The IoT market is currently dominated by companies like General Electric, Hitachi, and Siemens, which offer their own proprietary systems.

Businesses participating in Toshiba's new platform will not have to design their own services from scratch. Prototypes can be developed in one or two days by combining products from other companies, reducing the time needed for commercialisation.

The group will follow Amazon.com's model, which offers connection kits to manufacturers developing smart devices that use the company's Alexa artificial intelligence tech. Over 85,000 products have emerged through the program. Backers of Toshiba's initiative say it could help combine existing technologies in new ways, such as placing weight sensors in front of museum artwork to automatically start offering guidance when visitors are detected, and houses that activate their own lights and air conditioning at the turn of a key.

The diversity of the alliance's prospective members shows how the arrival of faster 5G wireless networks is stimulating innovation across traditional industry lines.

Toshiba will also develop a website for consumers that will display products developed by alliance members. Shoppers will be able to mix and match offerings even if they possess no programming knowledge. Companies and organisations in the ifLink community will pay annual fees between 30,000 yen and 3.6 million yen ($277 to $33,260) depending on their size and other factors.

SECUTECH THAILAND 2019 DRAWS TO A CLOSE AFTER INAUGURAL 'SMART CITY SOLUTIONS WEEK'

Displaying a collective enthusiasm to build a safer future, 8,576 industry professionals journeyed from all corners of Asia to attend the 7th edition of Secutech Thailand, which finished its four-day run on 31 October. With smart city solutions as a core theme, exhibitors and visitors alike were united in their consensus that the Thai security market is full of potential, particularly due to the government's commitment to smart city initiatives.

Positive sentiment also surrounded the successful synergies created between Secutech Thailand and Digital Thailand Big Bang, which were held alongside each other for the first time this year. Under the banner of 'smart city solutions week', the two fairs together with Thailand Lighting Fair and Thailand Building Fair created a one-stop shop for a wide variety of smart city solutions.

At the conclusion of the show, Ms Regina Tsai, the Deputy General Manager of Messe Frankfurt New Era Business Media Ltd, said: "We are delighted that Secutech Thailand has once again built bridges for important business connections to be made. The introduction of new show elements such as the Zhejiang Smart City area, as well as pavilions from Korea, Singapore, and Taiwan has connected the market with innovative products that can solve important security, fire safety, and smart living challenges. What's more, our successful collaboration with the Digital Economy Promotion Agency to run Secutech Thailand and Digital Thailand Big Bang concurrently has helped to further build the profile of Thailand's growing smart city scene."

More than 280 exhibiting brands participated at Secutech Thailand, with many commenting favourably about the connections that they made at the fair. "Every year that we attend Secutech Thailand we notice a different scale, and our company uses the platform to release a different high-level solution," said Mr Jeff Yang, the CTO of ZKTECO Thailand. "This year, we are showcasing our 'one-face' AI facial recognition technology. Many visitors have come to our booth and their feedback has been very good. Interest is coming from many different industries. We have met with system Integrators, government officials, and interestingly yesterday we met with two visitors from banks."

Tasked by the government to lead Thailand's digital transformation, the Digital Economy Promotion Agency has said that public and private sector collaboration will be crucial to achieve the government's smart city goals.

With government officials from both Thailand and the wider ASEAN region in attendance, Secutech Thailand's exhibitors had the opportunity to showcase their innovative smart solutions to a relevant audience. More than 20 VIP tours connected exhibitors with various government agencies, including: the National Municipal League of Thailand, the Mass Rapid Transit Authority of Thailand, the Fire and Rescue Department, as well as representatives from the UTAPAO airport authority, Suvarnabhumi Airport and Don Mueang Airport.

ISS, an exhibitor of video analysis software saw opportunities to promote their smart city and transportation solutions at the fair. Mr Nikolay Bushev, Vice President for international markets of the company said: "In the past we supplied our solutions to a smart region in Russia, where 15 different cities were linked to one monitoring centre, and at Secutech Thailand we have the possibility to show the Thai government our achievements. We are aiming to meet with traffic police and city authorities. Apart from these buyers we have noticed a lot of visitors from Myanmar, Laos, Vietnam, and Indonesia."

Mr Jonathan Chan, the Regional Product Manager of Singaporean company New DVR(s) was also enthused by the prospects in the smart city sector: "The government has been talking about establishing 100 smart cities in Thailand, and we can see many changes. The mindset of people in Thailand is very accepting and they increasingly know what the IoT is about. Secutech Thailand continues to be very supportive of the smart city scene. We can see that the organisers continuously attract relevant industry players that are looking for IoT solutions. We see bright prospects in Thailand for our open source IoT platform."

INSPIRO AND VERINT PARTNER TO IMPLEMENT INNOVATIVE VOICE BIOMETRICS

In partnership with Inspiro Relia Inc, Verint Systems Inc. has optimised the quality of RCBC Bankard's call centre operations with the implementation of Verint's innovative biometrics solution, part of its Identity Authentication and Fraud Detection (IAFD) offering. The combination gives the organisation high-level expertise and automated technology to help reduce costs and improve the overall customer experience.

RCBC Bankard Services Corporation, the credit card arm of Rizal Commercial Banking Corporation (RCBC), one of the largest universal banks in Philippines, collaborated with Verint on a landmark upgrade of their voice recording and biometrics systems.

Verint voice biometrics recognises the unique vocal characteristics of enrolled customers seconds into a live call, helping to reduce the number of security questions and average handle times. This faster authentication can reduce contact centre costs, help eliminate the need for security questions, and can provide an overall improved customer experience.

Mr. Simon Calasanz, RCBC Bankard President and CEO believes that the rollout of the solution was well timed and stated, "The implementation of voice biometrics improves our workflow and increases the security behind every single call. This is at a time when credit card fraud has become more prevalent."

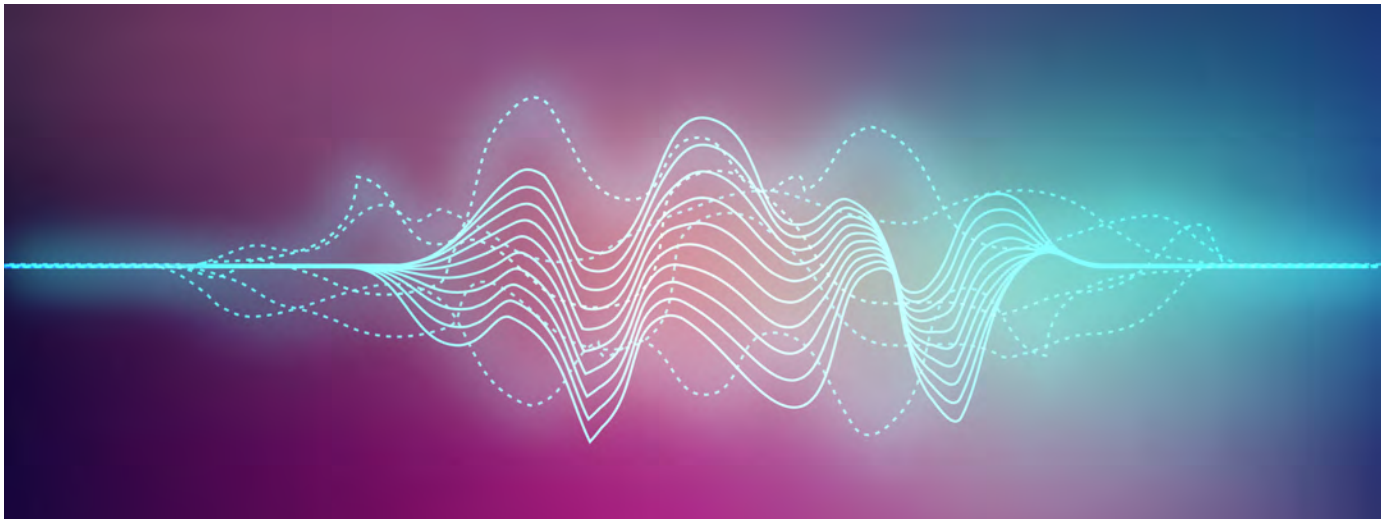
Calasanz continued, "Our service delivery is of utmost importance to our customers, and we are pleased to say that the upgrade to the system was executed to the highest degree. The Verint and Inspiro teams were well orchestrated and operations continued smoothly behind the scenes. Following the deployment, we expect a decrease in the number of security questions, and we will have the ability to provide assistance more quickly, with a reduction in average handle time."

Commenting on the successful partnership and project outcomes, Manish Shah, Vice President of Verint's Southeast Asia operations, said, "Understanding the RCBC Bankard's needs and a strong collaborative partnership with Inspiro were key to a seamless transformation of RCBC Bankard's back office operations. RCBC Bankard wanted to push the envelope with new modernised and automated technology that would help them to deliver higher quality customer service. Our local support capability and our voice biometrics technology was the winning combination that led to the successful execution and delivery of this project."

"Advanced voice biometrics is a positive disruption for our industry, and we are seeing greater adoption across the financial services industry," Mr. Shah added. "We look forward to working closely with our local partners to ensure they're providing the best customer service experience possible with best-fit solutions."

Mr. Mark Mistal, Inspiro's Chief Information Officer added, "Verint's capabilities within the contact centre space are well-established, and their best-in-class voice biometrics system delivers tangible enhancements to every single call and in real time."

Inspiro supports the customer engagement requirements of leading brands in the Philippines. Mistal continued, "As the customer service quality in the call centres get a new boost through technological advances, we see great value in our continued partnership with Verint."



Building Security For Smart Buildings

By CJ Chia

With the promise of greater convenience and increased sustainability, smart buildings seem an inevitability that many countries have set as a goal for a more connected infrastructure. Amidst this movement, it is important to consider the vulnerabilities that these buildings might have and make plans to reduce the risk of threats.

Try to picture cities of tomorrow and chances are, high-tech and connected infrastructure would come to mind. With the convenience that smart technology promises—coupled with tremendous room for growth—the advent of smart cities seems less a matter of "if", and more of "when".

As self-contained structures, smart buildings form the building blocks of the ecosystem for a smart city. By using integrated technology to regulate a building's ventilation, air conditioning, lighting, and security amongst other systems, the need for automation, control, and monitoring is addressed.

The result? Buildings which are able to automatically perform tasks like detect when a room is empty and turn off the air conditioning and lights. Throw automation into the mix and you can have a building which recognises the regular times during which a room is in use, cooling it down in advance for greater comfort.

Despite the huge potential in aspects like increasing efficiency and sustainability, smart buildings also create new vulnerabilities that would not exist in traditional buildings. As with any system that connects to the internet, a smart building is susceptible to cyberattacks.

As things stand, there is still plenty of room for smart building technology to be developed further to increase the benefits and reduce the openings through which the entire building's network might be compromised. With many cities globally making plans to move towards smart cities—Singapore's Smart Nation initiative for one—we can expect to see accelerated growth in this sector.

Smart Buildings For Increased Security

While many will think of digital concierges who can function as guides within a building (and other similar high-tech scenarios that make things more convenient for those using the building), smart buildings also have the additional benefit of increasing the security of a building.

By integrating security solutions into a building, the safety of the people inside and even in the surrounding area can be increased. For example, using facial recognition software together with compatible security cameras can help to identify suspicious persons throughout the building without needing as many security guards on patrol.

Automated security checkpoints are another great way to ensure that only those with proper clearance are able to access areas that might have sensitive information or equipment.

AI-powered cameras that can detect threats through behaviour like violent gestures, loud sounds, and even guns are already available. As more research goes into these technologies and machine learning, such solutions will become even more accurate, making them increasingly viable for different types of smart buildings. The tech goes beyond keeping people safe. Advances in smart building technology also mean that we can keep assets safer. For example, by installing temperature sensors at data centres and along production lines, we allow for the early detection of anomalies that need attention from an engineer or technician, creating the opportunity for an issue to be resolved before it becomes a major incident.

The possibilities don't end there. Using other smart sensors, different issues that can affect various assets can be detected early; using the 3D-mapping that the maritime industry has already started implementing, it will even become possible to investigate the issue in complicated machinery without having to first take it apart.

Other smart building technology that experts predict will be a trend in smart buildings include environmental monitoring, like wireless air quality sensors that will monitor the levels of harmful particles within a building, sending out warnings if it reaches a level that is unsafe for the people within.

Location-based services inside a building are also predicted to grow in use, allowing for greater convenience like allowing people to book a room and tracking the movement of those working or living within a building. With proper implementation, we can make keeping our buildings secure a lot more manpower-lean, allowing us to reassign skilled professionals to more critical positions.

Threats To Smart Buildings

Although smart buildings bring with them convenience and manifold benefits, there remains some weaknesses that might give you pause in embracing the idea wholeheartedly. With increased connectivity comes greater susceptibility to cyberattacks—when there is an entire network of devices

talking to each other, all it takes is one vulnerable device for hackers to gain access to the entire network.

These vulnerabilities are more than mere possibility. Take for example the Mirai botnet. On 21 October 2016, multiple major DDoS attacks in DNS services of service provider Dyn occurred using Mirai malware installed on a large number of IoT devices—many were using their default usernames and passwords. As a result of the malware gaining access to these IoT devices, several high-profile websites like Reddit, Twitter, Netflix, Airbnb, and GitHub were rendered inaccessible.

While there haven't been other attacks on a similar scale recently, Mirai has never quite gone away. And with its source code released to the public, copycat malware have popped up from time to time, posing a new threat that has to be patched before it has the opportunity to do any real and widespread damage.

DDoS attacks do more than cause websites to become inaccessible; they can pose a very real problem in smart buildings. Take an incident in eastern Finland, in the city of Lappeenranta for example. One weekend in November 2016, a DDoS attack caused the environmental control systems of two apartment buildings in the city to stop working, leaving residents in the cold.

The central heating and hot water systems in the buildings were attacked, causing the systems to reboot to fight off the attack. Instead of resolving the issue, this caused the systems to get stuck in an endless reboot loop. The attacks were apparently instigated simply because the systems were vulnerable, and similar attacks were reported to have affected other buildings in the country. These incidents highlight the potential weaknesses in a network where greater connectivity brings with it increased risk, and security vulnerabilities continue to plague building management systems despite these incidents highlighting the importance of greater security.

Protecting Smart Buildings From Cyber Attacks

With buildings inevitably becoming increasingly automated and more connected, it is more important than ever that building management firms start putting greater focus on cyber security. Currently, many smart buildings do not have a proper security policy in place to handle vulnerability reports. Security firms who find vulnerabilities have their work cut out for them finding the proper channels through which to report these issues so the smart building management can arrange for security patches to be made. And when this report is made, organisations sometimes react with apathy or outright hostility instead of working on a fix.

In order to maintain a smart building's security, it's important to implement the right practices. For one, all the smart aspects of the building should have their software updated regularly, including proper antivirus and firewall protection. It is also advised that if it is necessary for management to gain remote access to a building's systems, that this access be put behind a virtual private network (VPN) so that it's not as easily infiltrated. Introducing tiered levels of authorisation can also help to restrict the number of devices that gain access to various smart features and reduce the points that can be targeted by attackers.

Another aspect of security that is often overlooked is the need for clear regulations and guidelines that allow landlords, developers, and tenants to have a clear and consistent idea of what needs to be adhered to in order to maintain a building's security.

On a device level, it is important to ensure that each individual IoT device is kept secure. Measures like ensuring that a device's username and password has to be changed on the initial setup can make it more challenging for hackers to gain access to a device. In addition, it might be helpful for the real estate industry to look at and adopt some of the IT sector's practices. For example, implement robust testing cases to check both common and uncommon events and how it affects a device's software before deploying it within your building. Hackathons can also be useful in testing and finding vulnerabilities in a smart building network, while the use of AI and machine learning as an additional layer of threat prevention can leave cybersecurity professionals to focus on more unique threats and cases.

Other than prevention, it is just as important to ensure that a proper response is planned out in the event that the device is compromised. As with all things related to technology and the Internet, there will always be new threats that surface as cyber criminals seek to exploit various vulnerabilities for their own gain. Therefore, being prepared for the absolute worst-case scenario is paramount in the efforts to keep smart buildings secure.

Are "Invisible" Technologies The Key To IoT Payments In Retail?

Consumers seek easy, seamless experiences, without giving too much thought to the technology behind it. The payments industry should be delivering a frictionless customer experience that balances security and consumer expectations.

By Monica Eaton-Cardone, co-founder and chief operating officer of Chargebacks911

Here's the truth: the average consumer doesn't want to think about how IoT-enabled technologies work. If you picture the typical buyer, that individual probably loves the freedom and new experiences brought by the Internet of Things…but that doesn't mean they really care how we bring to market the technologies behind them.

Fortunately, we don't need consumers to consciously embrace IoT technologies to advance their use. Instead, we can take the approach of selling users on an experience and use the power of IoT to deliver it.

Everyday buyers are hungry for what we can call "invisible experiences." They want an experience enabled by IoT technology but without the need to be cognisant to the technology itself. This is very true of conducting payments, for instance. Buyers don't want to worry about how the technology enables a complex exchange between multiple institutions and accounts, nor are they interested in the ins and outs of payments clearing; they just want it to work.

It's true that invisible payment experiences are becoming a consumer expectation. This fact will impact retailers who are unprepared to meet customers' ever-more stringent demands. But, if managed well, it could open the door to some fantastic new opportunities.

Bringing The Invisible Ideal To The Market

Data recently published by Gartner projects that, by 2020, we'll have 21 billion devices connected to the internet. That's a mind-boggling 21 percent increase over 2019. The more seamlessly these devices are integrated alongside one another, the better the experience we can offer consumers.

Developing technologies present a lot of divergent opportunities to integrate IoT tools into different experiences. To demonstrate, one of my favourite illustrations of the invisible experience principle at work is Disney's MagicBand technology.

With this simple wrist device, you have no need to worry about keeping track of park tickets, passes to skip attraction lines, hotel keys, or even your payment card. You can effectively leave your wallet in the hotel room and use the MagicBand to manage all your needs. It's cardless payment technology, but it's integrated into a much broader customer experience; you might even say that it works like magic.

Amazon Go is another great example of how we can employ IoT technology to deliver an invisible and seamless customer experience. When the company unveiled their "Just Walk Out" technology to the public back in 2018, the general attitude seemed to be sceptical yet curious. Nearly two years later, the company's expanded their concept to 17 additional stores in four cities.

In an Amazon Go store, the customer simply grabs what she wants and leaves. There's no need to checkout; the items are automatically added to an Amazon cart via the mobile app, then charged to the user's account. It doesn't get more seamless or invisible than that in terms of payments technology.

IoT Payments: Balancing Security And Consumer Expectations

As with any new technology, we can't rush into the invisible approach to IoT payments without the right protocols in place. Security is—and should always be—a primary concern.

It's a challenge to reconcile the need to make payments technologies as invisible as possible, while also delivering security that meets critical standards. As the line between brick-and-mortar and eCommerce grows increasingly blurred, the problems inherent to one channel bleed over into the other. Bringing card-not-present commerce into stores invites many of the same issues we have with eCommerce fraud, which is a rampant problem for online sellers.

One option is to incorporate biometrics on a more integral level. Asking

customers to provide a thumbprint or a facial scan to authorise payments does add a small amount of friction to an otherwise invisible process. It's also true that some customers could be turned off by the idea of providing a biometric reading. Nonetheless, going with a biometric-first approach to authorisation offers dual benefits: it acclimates buyers to the new technology while also providing strong authentication with minimal friction.

Just as important as the technology, though, is how we manage consumer expectations. I believe that we can get out ahead of those wants by defining consumers' expectations ourselves. This means not overpromising on what we can do.

We like the idea of an invisible process, but even then, it's not truly "frictionless" or invisible. There must still be checks in place to ensure basic security and authentication. While we don't want to add unnecessary roadblocks between merchants and customers, we also shouldn't foster an expectation of totally invisible and frictionless commerce.

There's a balance to strike when it comes to IoT payments. Only with a keen eye for both streamlining the customer experience and covering one's bases from a security standpoint can merchants optimise the experience they offer consumers.

The Future Of Physical Retail: Connected Devices And Connected Shoppers

Brick-and-mortar retailers are experimenting with IoT technology, from smart mirrors and tablets in fitting rooms to VR headsets and beacons on the retail floor, to transform the shopping experience and drive more offline sales.

By Mike Leibovitz, Senior Director of Product Management at Extreme Networks'

These cutting-edge IoT technologies are defining the stores of the future. But what's often overlooked is that these novel, customer-facing innovations all depend on foundational backend systems.

Putting The "Smart" In Smart Fitting Rooms

Smart and connected fitting rooms are on the rise in major retailers across the country. For example, Ralph Lauren outfitted its flagship store in New York with smart-mirror fitting rooms so shoppers can request different sizes and colours, view product information and even adjust the room lighting all through the connected mirror.

AR and VR technologies also introduce new possibilities for consumers to interact with products and companies in personalised and exciting ways. Timberland deployed AR mirrors in their storefronts to attract and engage foot traffic. Their smart mirror enables those passing by to virtually "try on" various outfits and even share their experience on social media.

These examples illustrate the rise of experiential retail, and both smart fitting rooms and AR devices depend on a fast, reliable internet connection in order to function properly. The storefront magic mirror loses much of its appeal if it requires shoppers to wait several minutes for the images to load.

Highly available, flexible and scalable Wi-Fi connectivity is imperative for supporting these bandwidth intensive IoT, VR and AR applications. Retailers can use automated Wi-Fi radio frequency management to proactively identify and mitigate issues before they occur, which ensures a high quality of service for shoppers. As a result, consumers will

experience minimal latency and reliable connectivity when using the experiential technology.

Making Payments Mobile And Secure

Consumers expect the in-store checkout experience to be as seamless and efficient as shopping online. Recognising this, many retailers are deploying IoT payment devices such as tablets, smartphones and smart carts to expedite the checkout process for consumers. In turn, this can also help retailers streamline their in-store operations and resources.

Automated checkout can reduce cashier staff requirements by up to 75%, resulting in savings of $150 billion to $380 billion per year in 2025, according to McKinsey. One critical concern that could jeopardise the successful execution of a mobile payment strategy is security. Ninety percent of consumers lack confidence in IoT device security, including point-of-sale (POS) devices, according to Gemalto. Verizon's 2019 Data Breach Investigations Report found that while breaches involving POS have declined in recent years, attacks against ecommerce payment applications are on the rise, accounting for 81% of breaches.

As the use of mobile-based payments and connected devices grows, so too does the attack surface. IT managers must ensure their in-store network includes a mix of threat detection, protection, and surveillance to prevent the exposure of confidential consumer and business data.

Furthermore, most retail IT teams are small with limited resources, and they are responsible for managing multiple retail locations across different regions. A network equipped with machine learning and proactive AI functionality to identify anomalies and potential threats can help augment human intelligence and reduce the time spent manually monitoring for security vulnerabilities.

Connecting To The Connected Customer

There's a lot of hype around net new IoT devices that retailers are deploying in their stores. But it's not just businesses that are more connected; it's customers, too. Buyers today increasingly shop with mobile phones, tablets, smart watches and other wearables, putting real-time data on discounts and competitive pricing at their fingertips.

According to Salesforce research, 71% of shoppers say they use their mobile devices in stores and eMarketer reports that 69% percent of consumers look for reviews in-store on their phone before approaching a retail associate. That leaves retailers a narrow window of opportunity to meaningfully engage shoppers who otherwise may opt to purchase from a competitor.

The good news is this proliferation of devices on the network also creates a proliferation of valuable consumer data, which retailers can leverage to deliver more personalised offerings and customer experiences. For example, Macy's uses beacon technology so that when a customer opens the Macy's application while shopping, the application sends targeted promotions and contextual information based on where the customer is in retail locations. In many ways, this allows retailers to meet customers where they're at, and curate more touchpoints throughout the physical and digital shopping experience to achieve unified retail commerce.

It's important to remember that the network edge is now a cornerstone of brick and mortar retail stores. It's the point where an organisation and its customers meet; it's where users engage, mobile transactions occur, and IoT devices connect and are managed. Retailers can apply analytics to the data coming over in-store wireless networks to understand customers' preferences and make offers to them that are highly contextual and catered to their specific needs. Analytics can also be used to inform location-based services, RFID, and electronic shelf labelling to reduce friction in a shopping journey and create impactful experiences.

Modernising Brick And Mortar By Connecting The Dots

As we head into the busiest shopping season of the year, it is an opportune time for retailers to evaluate how their in-store technology elevates or hinders the end-to-end customer journey. Whether it's high-tech experiential IoT devices, mobile POS systems, or your customer's smartphone, remember that the network is critical to a seamless in-store experience.

Can Smart Parking Help Save The Brick-and-Mortar Retailer?

Smart parking could be key to bringing back customers to physical stores by providing seamless parking and data that can improve business KPIs, improve the customer experience, and reduce emissions.

By Thomas Hohenacker, CEO & President of Cleverciti

The rise of connected devices has shifted the conversation across a number of industries, and retailers are feeling the crunch. As the Internet of Things (IoT) is widely adopted—25 billion devices are expected to be connected by 2021, according to a 2018 Gartner forecast—it's driving efficiencies across numerous industries, and retail is most well-positioned to benefit.

While online retailers have previously been the leaders in adopting new technologies, IoT presents enormous opportunities for traditional brick-and-mortar retailers. One such opportunity is reinventing the parking search. Shopping at a brick-and-mortar location starts with looking for parking, and the average driver wastes 12 minutes finding a spot at the average mall. With artificial intelligence (AI)-powered IoT devices, the parking search time can be dramatically reduced, helping to reinvigorate brick-and-mortar retailers.

Smart Retail – Customer Satisfaction

A retailer's parking situation is the first and last impression made on a customer. A negative experience searching for a space can set a negative tone for the entire trip, reducing time spent shopping and negatively impacting the brand experience. The same goes for when a customer is leaving the store: a productive and enjoyable shopping trip can be soured by forgetting where the car is parked or having to spend extra time trying to exit the area.

Smart parking technology that guides drivers directly to an open parking spot eliminates the frustration and increases

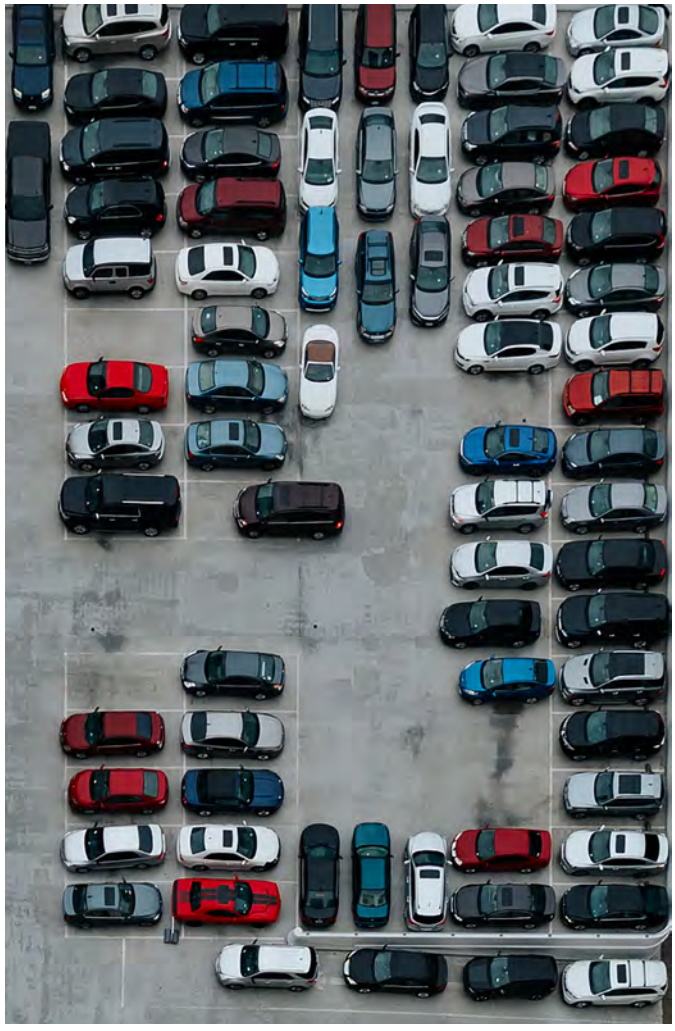


Photo by Ivana Cajina on Unsplash

customer satisfaction with their entire shopping experience. Overhead sensors mounted on lampposts can gather information on available and occupied spaces in real-time and then transmit that data to digital signage that easily guides drivers.

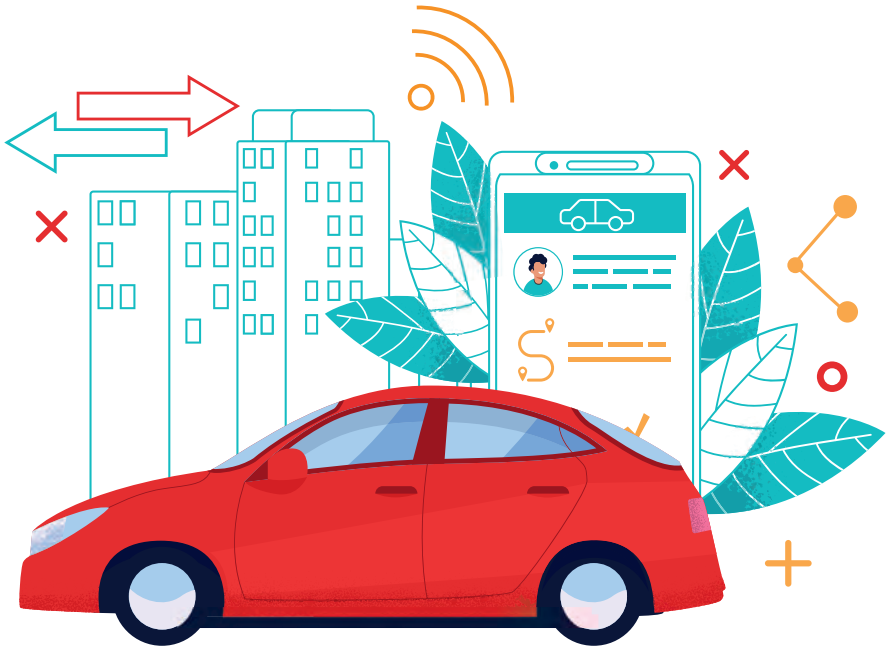
Advanced Data For The Retailer

Customers aren't the only ones that stand to benefit from smart parking technology. Parking operators can gain increased visibility into their operations through real-time data collected within the backend of the software platform. This information can provide operators with information such as how long a car has been parked or if there are any parking violations such as unauthorised use of loading zones or handicap parking. This empowers the retailer to better understand one of their greatest assets and make quick and educated decisions if needed.

This data also goes beyond the ability to analyse parking trends and can help management learn more about their organisation and marketing efforts. For example, the average length of stay of customers at the retailer can indicate which marketing strategies are working and when the best times are to promote sales.

Creating A Rewarding Experience

Many large retailers leverage credit cards or rewards programs to provide a discount, bonus or gift to customers



based on their spending habits, but this type of initiative doesn't have to be limited to shopping. Imagine going to a shopping centre during the busy holiday season and pulling into a parking spot that was specifically reserved for you ahead of time.

Advanced smart parking technology facilitates the creation of temporary parking permits that streamline management and guidance for surface lots and parking garages. Through a single card and mobile application, customers can receive a message detailing which spaces are available as they approach a lot, reserve a space before arriving and even make payments if necessary. This seamless process will encourage drivers to choose retailers that care about most.

Reduce Emissions

The search for parking also creates an incredible amount of pollution. For example, in a shopping mall with 1,000 parking spaces, shoppers typically drive the equivalent of 75 times around the world each year simply searching for a spot. This also dumps around an estimated 524 tons of unnecessary CO^2 emissions into the environment. Smart parking using live data collected from connected technology can reduce the search for parking by at least 30 percent. Not only can the retailer feel great about its part to save the environment, but a report by Nielsen found that 66 percent of consumers are willing to pay more for sustainable goods, so it's likely that they will also pick a shopping centre that has actively chosen to reduce its carbon footprint.

In these times of unprecedented challenges for brick-and-mortar retail, adopting advanced new technologies like smart parking can transform the guest experience from one of hassle and stress, to seamless and positive, while gaining data on customer behaviour. Smart retail solutions might just be what brick-and-mortar retailers need to turn around.

Wireless Sensor Solutions That Solve Retail Problems

Wireless sensor technology enables a new level of automation that has major implications for many sectors. One sector that is already benefitting significantly from this next-gen technology is the retail space. Here, we highlight major applications for wireless sensors in retail and showcase the versatility of the technology.

Article reproduced from IoT for All

Over the next decade, billions of Internet of Things (IoT) devices will flood the market and change many aspects of our lives forever. These IoT devices are powered by wireless sensor technology, which enables us to create networks of interconnected objects that can exchange information independently. With wireless sensors, we can automate processes that would otherwise require human intervention.

One of the sectors that is already being transformed by the IoT and wireless sensors is the brick-and-mortar retail space. Retailers can use wireless sensor networks to create better in-store experiences, enhance security, and improve operational efficiency in many ways.

Already, there are many examples of how wireless sensors are being deployed in retail settings. Below are a few use cases that showcase the versatility of wireless sensor technology.

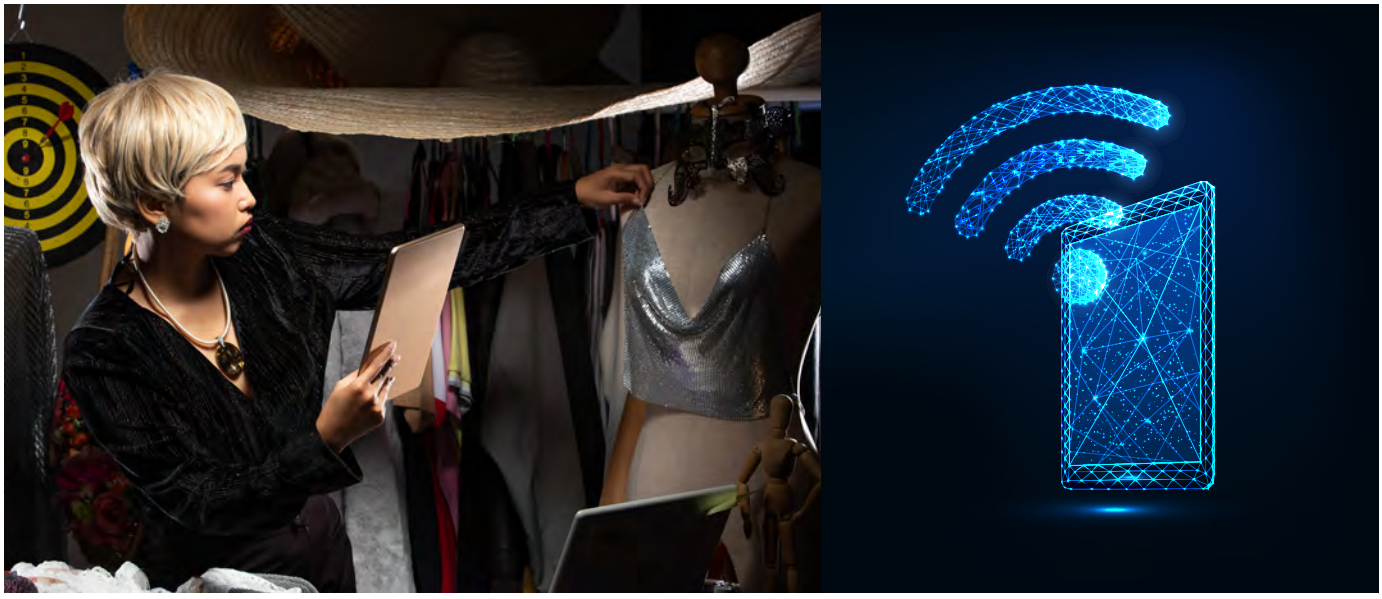
Improving The Onsite Experience

There are a variety of ways retailers can use wireless sensors to improve experiences for both customers and employees. One particular class of sensor, the wireless pushbutton, has several potential applications inside retail locations. Wireless pushbuttons can be installed in bathrooms and configured to send messages to janitorial staff when pressed. With the simple click of a button, shoppers could alert when bathrooms need to be cleaned or equipment is out of order.

Pushbuttons could also be installed throughout large merchandise areas so customers could notify sales representatives when aisles need to be reorganised. Large department stores, such as Macy's or Nordstrom Rack, could use pushbuttons to help maintain large areas that are challenging to manage throughout the day.

Wireless pushbuttons can also serve as low-cost silent alarms. Employees could easily notify security or law enforcement teams by pressing the sensor when they feel threatened by individual customers.

To help maintain comfortable internal environments, retailers can use wireless temperature sensors and humidity sensors to monitor air quality. For example, temperature sensors can be deployed in superstores that have refrigerated and non-refrigerated areas. Temperature sensors can alert if temperatures fall below a pre-set level,



thus indicating a possible refrigeration failure. Or, they can be placed throughout electronics sections to monitor units that may overheat.

Wireless air sensors are effective for those who need to monitor humidity closely. Retailers with garden operations need to ensure the right conditions exist for all types of plants. Humidity sensors are also useful for preventing mould in areas with poor air circulation.

Those with major inventory and warehouse operations might use wireless temperature sensors to ensure that safe working conditions exist for employees. Temperature sensors can be installed and programmed to detect possible cooling system failures.

Bolstering Surveillance And Security

Wireless sensors are effective for supplementing security teams and onsite surveillance. There are different types of wireless proximity sensors that can detect movement or opening and closing events at specific access points. A retailer might want to deploy proximity sensors where valuable merchandise is stored or where money is held. These sensors could alert security teams whenever movement is detected.

Wireless window sensors can be placed on external access points that burglars may use to enter buildings unnoticed. Wireless door sensors can be installed on cabinets, lockboxes, or rooms that need to be watched closely. Relying on automated wireless messaging allows retailers to reallocate security expenses and maintain secure premises in a low-cost manner.

On the supply chain side, wireless acceleration-based sensors can be attached to valuable assets and configured to send alerts when items are moving. A retailer might want acceleration-based sensors on high-cost items to ensure no products move outside of sales or expected transfers.

Protecting Retail Facilities And Operations

Wireless sensors help manage critical retail systems and operations. For example, wireless water sensors are valuable for protecting against leaks, plumbing issues, and pump failures that could wreak havoc on the inside of retail stores. Water rope sensors can cover significant square footage and notify facility managers instantaneously of liquid spillages.

These alerts are especially valuable when issues arise in server rooms or in data centres where massive amounts of information are stored. Water leak sensors are also able to detect frozen water, which is helpful for identifying vulnerable pipes at risk of bursting.

Wireless vibration sensors are used to detect early signs of equipment failure. By installing vibration sensors on stationary equipment, retail facility managers can identify when systems may be malfunctioning before they are beyond repair. These low-cost sensors can result in thousands of dollars of savings and last for several years on a single battery charge.

Wireless Sensors Bringing Next-Gen Technology To Retail

Wireless sensor networks and IoT have helped usher in a new era of automation for businesses of all types. In the retail world, there are many applications for wireless sensors that support facility managers and operation leads daily. Looking to the future, expect to see more and more wireless sensors enhance experiences at major retail locations and improve onsite efficiencies.

Data Interpretation Plays Pivotal Role In Retail Loss Prevention

Combining security technology with business data is paramount to creating a comprehensive LP strategy.

By Bruno Mota and Kelly Del Fuoco, co-founders of Pembroke Loss Prevention

In today's machine-driven day and age, having the latest and greatest security technology seems like the end goal. We all know whatever is newest and most comprehensive gets the top billing at tradeshows. Even a quick Google search on "top security cameras" boasts about those with Wi-Fi connectivity, cloud storage, and smartphone app capabilities.

However, though we now have the best security technology that has ever hit the market, businesses across the world are still facing losses. These losses may be monetary. They may refer to high employee turnover. They may encompass leads that are slipping through the cracks. So where is the disconnect between technology and results? Shouldn't top technology hinder losses automatically?

The fact is, it's not that simple. You can have the best security technology in the world, but without the proper data and analytics strategy in place, it won't do you any good. A well-planned strategy will transform your security

technology from an eyes-in-the-sky piece of machinery to another "team member" that increases sales, improves employee productivity, and streamlines operational efficiency for optimal business success.

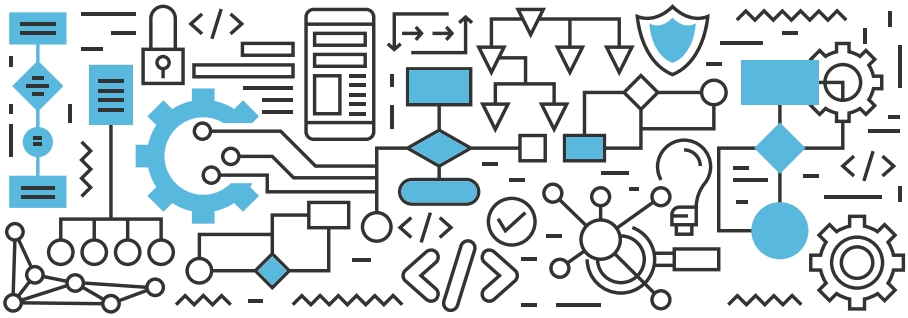
The Importance Of Data

Data and algorithms are widely used terms today, but ten years ago when we began our journey in the loss prevention industry, those words were reserved for mathematicians and investment bankers. We recognised the benefits these numbers have for narrowing down on a business plan and identifying bottlenecks, regardless of the industry. Where sales are involved, algorithms can be used to best determine where to begin tackling loss prevention issues. The best part is that this data can be garnered directly from the technology businesses already have on hand, like security cameras, point-of-sale transactions, financial reports, and more.

However, sifting through this data is another beast entirely. Many companies new to this process think that just having the data on hand is enough. This can lead to the age-old trap of bypassing the tedious part: watching video and analysing trends.

These hundreds and thousands of data points paint a picture, and though algorithms are used to better sort this data quickly, the anomalies or "red flags" need to be examined closer. It's the beast of burden, but well worth the while. There is simply no way to quantify the investigation any quicker. Missing this data doesn't evaporate these red flags from the bottom line. A strong strategy requires the data to be reviewed with care and diligence, no matter how much you have to sift through. Ultimately, this data will serve as a road map to make your trip a little easier.

This is why simply installing a top-notch security camera isn't enough. The data it provides a business is plentiful and the benefits are



immeasurable, as long as business owners and decision-makers know how to interpret it.

Bringing Technology And Data Interpretation Together

When security technology and business data are combined, a loss prevention strategy is born. Loss prevention is no longer just people chasing after shoplifters. It now encapsulates an array of areas. As mentioned before, these losses can include anything from employees committing theft (cash, merchandise, or time), but also the biggest loss of all: customers.

Using the best security technology available today in cameras and software allows entirely new methods to exist for customer retention, such as online customer reviews. We now have the ability to read a customer review on Yelp, Google, or Facebook and pinpoint the exact specific event on camera. At times, this also reveals trends on whether the customer review is not only accurate, but also prevalent. The customer experience needs to be the number one priority for any business and with how far technology has come, we can have multiple cameras running at once to see the exact flow taking place like a well-oiled machine. Better technology, better cameras, and better data-sourcing allows us to diagnose a problem in the machine right away.

What's more, this strategy can now increase management's response time. If a customer has a complaint or an employee brings up an issue, with access to state-of-the-art camera systems and sales data, we can pinpoint the exact instance or similar instances and review for trends. Before, a customer complaint could be viewed as a headache that can't be proved, or an employee raising a concern would be difficult to determine. Now, as long as they know how to interpret the data a security camera or similar technology brings us, management can immediately address all questions and concerns knowing the data and footage are there to paint the picture clearly. By zooming in on the bigger picture, the issue can be resolved within minutes and avoided for the rest of a business's successful lifetime.

These are just a few examples of many on why you need a proper data and analytics strategy in place to make the most of your security technology, and what a strategy like this can do for you. Ultimately, if you don't have a strategy in place, it doesn't matter if you install the top piece of technology on the market, how much you spent, or how small and lightning-fast the microchip is. Your technology will do nothing useful for you. Using security technology to tell your story can help your business turn loss into opportunities, but only when coupled with a proper data interpretation strategy. Don't let your technology be another loss in your business plan. Make it work to your advantage and see how much success it yields.

Five Ways The Travel Industry Is Embracing IoT

Airlines now allow smart device flight check-ins, car rentals use IoT to monitor their fleets, and IoT-enabled luggage trackers make sure your stuff never gets lost again. Welcome to IoT for travel.

By Kayla Matthews, IoT for All

The Internet of Things (IoT) refers to the growing assortment of connected devices – many of which you may already own. Industries from agriculture to entertainment could benefit from the possibilities IoT offers.

The travel industry is also embracing IoT technology and uses it in innovative ways.

Letting You Check Into Flights With Your Smart Speaker

Amazon's smart speakers introduced the world to a virtual assistant called Alexa. With Alexa, you can order pizzas, book taxis and more. United Airlines now allows smart device flight check-ins via Amazon and Google Home smart speakers, plus the Fitbit Ionic smartwatch. You can also use the feature to find out about flight statuses or the amenities available during your journey.

Airlines began offering advance online check-in services several years ago, and this improvement aligns with the increasing adoption of smart speakers in the consumer market.

While soon-to-be vacationers are in the middle of doing last-minute essentials like packing their toiletries and writing care sheets for their pet sitters, the smart speaker feature is a quick and convenient way for them to get ready to fly.

Tracking Rental Cars And Streamlining Customer Processes

Once many people arrive at their destinations, they head to rental car outlets and get their temporary modes of transportation. Hertz is among the brands that use IoT to monitor their fleets. One service, called Hertz 24/7, allows renting cars by the hour with an accompanying app. The service even allows renting box trucks for transporting large items like furniture.

Each renter gets a keyfob that works with a reader behind the windshield. It opens the car for the first time, then allows a person to get inside and grab the keys that are in the ignition. There are also voice services inside the cars that connect people to a centralised contact centre in case they have any questions.

It's not difficult to see why advancements in IoT benefit customers and rental agencies alike. Services like the one Hertz offers allow people to rent cars at any time—not just within business hours. Plus, car rental brands can track vehicles if renters don't bring them back by the agreed-upon time.

Helping People Search For And Book Hotel Rooms

If you're a long-time traveller, you probably remember a time when booking a hotel room meant either calling the front desk before arriving or showing up and hoping for the best. HotelTonight is a website and app for hassle-free hotel room bookings looking to remove this obstacle to smooth travel.

HotelTonight helps you embrace spontaneity by allowing same-day reservations along with the usual advance booking option. Some of the accommodation choices you'll see in the app feature limited-time discounts in addition to the app's already appealing offers. Their HT Perks program gives you even deeper savings after spending at least $250 on rooms booked through the app.

Many people can't imagine parting from their smartphones. According to a Pew Research Centre study, 46 percent of respondents said they couldn't live without their device. Besides keeping you in touch with loved ones, smartphones and apps like HotelTonight help you book hotel rooms quickly after browsing to see which one works best for the trip.

Giving Travellers the Details About Their Lost Luggage
There's nothing like the heart-sinking feeling of realising you made it to your destination, but your bags got lost somewhere along the way. Until recently, people in this situation were at the mercy of baggage claim workers, who usually couldn't tell a frazzled traveller where a misplaced suitcase was and when to expect it back.

Things have changed, thanks to IoT-enabled luggage trackers. For example, people can refer to the associated app and tell the luggage counter agent they can see the bags never got onto the departing plane during a Boston layover. Then, the airline professional can use this information as a starting point to track the bag and reunite it with the owner.

For nearly $400, you can also get a Louis Vuitton luggage tracker that alerts you if someone opens your bag after you check it. These solutions put the power in your hands to discover the whereabouts of your stuff, so you can spend less time wondering and more time enjoying your travel.

Providing Parking Information

Research shows motorists waste time, money and fuel looking for vacant parking places. Trouble finding one could result in you having to rush too much to catch a plane, park farther away than you want or pay a higher-than-average rate to park out of sheer desperation. However, the benefits of IoT parking technology assist travellers and parking lot managers alike.

On the consumer side, a person could book a parking spot in advance, then get guided to the exact row and level of a parking garage. The companies that offer parking services could see metrics from IoT sensors that show the peak usage times, the average number of cars that enter and leave per hour, when a garage becomes full and more.

It's Easy to Become A More Connected Traveller

The examples on this list show the numerous ways you could have smoother, more enjoyable travel by using IoT tech. Since so many brands and companies are exploring how they can help customers while supporting their bottom lines, you have plenty of options to ponder before making investments in connected technologies.

Finnish Biometric Identity Plans For Seamless Air Travel

Finnair and Finavia explore options for automatic digital identification and authentication of air travellers.

By Alex Cruickshank, ComputerWeekly.com

Working on the assumption that air travel will continue to grow in the future, two Finnish organisations have carried out exploratory investigations into the possibility of simplifying the identification and authentication of passengers, for air travel in Finland and potentially elsewhere.

Finavia, formerly known as the Finnish Civil Aviation Administration, is the Finnish government organisation responsible for overseeing air travel within, to and from Finland's 21 airports. Working with Finnair, the Helsinki-based flag carrier and largest Finnish airline, Finavia ran a pilot trial earlier this year to determine the feasibility of certain new approaches to simplifying passenger identification.

The two organisations worked with a digital identity pilot initiative called Sandbox of Trust, which is aiming to create SisuID, which acts as a portal or aggregator to a variety of different identity documents.

Using facial recognition, this potentially means that travellers need never show their identity documents throughout the entirety of their journey, with facial recognition providing authentication every step of the way. Crucially, it's the user who decides which ID information is shared through SisuID.

According to Jouni Naskali, head of technology and cyber security at Finnair: "As the number of air travellers grows, the industry must find solutions for improving the current processes, and passenger identification is one of the most repetitive, time consuming processes at the airport. Biometrics has potential for enhancing this process, and Finnair actively explores with different stakeholders how the travel experience could be made more future proof, convenient and secure for our customers."

Finnair and Finavia recognised the importance of placing the passenger at the centre of the process, especially when it comes to matters such as privacy, data security, and consent. For example, from a practical and legal perspective, who would be responsible for the biometric data at each stage of the authorisation process?

Heikki Koski, chief digital officer of Finavia and vice-president of Helsinki Airport, said: "We are seeking a model which would benefit passengers most. A solution where the data controller would be a digital identity platform provider utilising MyData principles would be ideal as it would expand the use of digital identity outside Finavia airports.

"In 2017, we carried out a small-scale test of a biometric identification together with Finnair," said Koski. "The results we got were positive. As many as 30 out of 37 interviewed passengers replied that they would join further pilots or implementations. The rest said they might join. No one stated that they would not join in future."

The 2019 pilot determined that fully biometric authentication could significantly improve passenger flow and also the subjective travel experience for people flying within Finland. However, no customers were involved in the pilot, which was more a proof of concept project to identify pros and cons of the proposal.

Naskali at Finnair said: "In 2019 we engaged in SisuID piloting together with Finavia, and the focus in this project was in understanding technical and passenger flow implications in biometric enabled passenger process. We are also taking part in the biometric boarding at Los Angeles airport as of last summer, and in 2017 we conducted a proof of concept pilot with facial recognition technology in identifying Finnair frequent flyers at Helsinki Airport in collaboration with Finavia."

So where does this leave the concept? As the pilot findings note, there are no technical or legal obstacles to implementing fully biometric authentication on a per-traveller level, at least within the Schengen area. That's true even if using a mobile app with user registration.

However, it's a different matter when it comes to actually scanning passengers as a group, especially if not all of them have consented to the use of biometrics. In other words, there's a legal issue relating to the mass scanning of people who may have not signed up to the scheme.

Data Protection

In accordance with GDPR and other data protection/privacy regulations, there's also work to be done in deciding who controls and processes the data. This isn't easy to resolve, since the data "belongs" to the user, at least in principle. There are also additional considerations when handling the data of passengers travelling outside the Schengen area. In fact, privacy and data security, rather than technology, are likely to be the biggest stumbling blocks to applying the pilot on a large scale, which is partly why there's currently no timetable for implementing seamless whole-journey biometric passenger authentication.

"The pilot we conducted together with Finnair was the very first steps," said Finavia's Koski. "The aim was to gather insights into biometric identification as a part of our aim to ease and smoothen air travelling with seamless and fast passenger processes. There are still many open questions like privacy aspects."

In other words, more research is needed. Koski said in addition to privacy issues there are other legal topics that have to be investigated. "We need more information and data about how biometric systems change passenger flow and the airport operations."

It will therefore still be some time before Finnish air passengers can stroll through an airport, their documents in their carry-on luggage, their phones in their pockets, being identified every step of the way by facial recognition, with no need to show ID cards, tickets or passports.

Digital Experience Projects Balance CX, Data Privacy Concerns

Users want hyper-personalised, convenient experiences when they shop or stay at hotels, but brands must balance the thin line between convenience and invasion of privacy.

By Bridget Botelho, TechTarget

There may be nothing more frustrating after a long day of travel than getting to your hotel room, swiping the key card and seeing a red light instead of green.

That's one of the many inconveniences Hilton hopes to solve through its digital experience strategy, called Connected Room. The IoT technology allows guests to use their mobile device as their in-room remote, lighting control, a digital key and as a remote to set or change their room temperature.

"Our app is an all-in-one command centre that empowers customers," said Naveen Manga, vice president of customer journey technology and delivery at Hilton Worldwide, during a session at Gartner IT Symposium here this week. "It provides choice and control."

The company has more uses in mind for Connected Room technology, and continues to add partners, such as Netflix, to customise the digital experience. For example, Hilton could monitor the battery status of the room door lock

systems to ensure guests never see that blinking red light when they arrive. It's a simple use case that could have a profound impact on customer experience, he said.
The IoT system is in a limited number of Hilton's 5,500 worldwide properties so far, but it's being rolled out worldwide. The technology behind it is a proprietary in-room appliance that sends protocols to other devices in the room using Bluetooth. It's scalable "from edge to core," and secure across boundaries, according to Manga. "Having a proprietary device in the room that's fully redundant, and a secure system that we built on open standards, allows us to control it and build it out," Manga said.

Earlier this year, Disney rolled out technology called Interactive TV (ITV) to personalise the experience for guests of its Coronado Springs Resort here. Upon arrival in the room, the guest's name is displayed on the screen with a welcome message. Guests can connect their personal devices to the screen and see their vacation plans, including any photos linked to their accounts. This digital experience technology will be rolled out to all Disney World resorts in the years ahead.

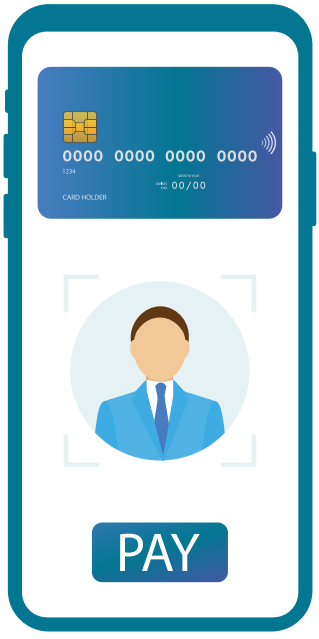
For every person who appreciates the convenience of hyper-personalisation from Hilton and Disney, there is someone who finds it "creepy." A group of attendees here said they wouldn't want to see their name automatically appear on the hotel room TV screen or have their personal preferences connected. Among them is Thierry Beniflah, a business relationship manager who works at a global human services organisation. He said data collection is too ubiquitous, and he gladly trades convenience for personal privacy.

"I don't want my data to be collected and sent somewhere else. There is no way you can control the way the data is used once it's collected," he said. "So, I lie shamelessly every time I'm asked to fill out my personal information online."

The 'Privacy Paradox'

While plenty of people say they don't trust companies to use their data ethically, many -- particularly millennials -- are willing to share their personal information in exchange for convenience and personalised experiences, according to a 2019 Gartner survey. This "privacy paradox," as Gartner calls it, marks the inconsistency between customer concerns about privacy and their desire for a personalised digital experience.

Take facial recognition payment, for instance, which allows consumers to simply look into a camera to approve a



transaction. In China, facial recognition payment systems have already been adopted and use is accelerating, but the AI technology isn't likely to expand to regions where such technology is seen as an invasion of privacy, according to Van Baker, a Gartner analyst who led a session on trends in digital experience through 2020 here this week.

"As far as [Chinese citizens] are concerned, it's the ultimate in convenience," Baker said during the session. "In other areas of the world, [facial recognition] is viewed as the ultimate invasion of privacy."

Companies such as Hilton have to be sensitive to cultural views and provide the right type of personalisation for customers, while allowing them to safeguard their personal data.

"We allow our customers to opt in or out, and see where we store the data, what we store and we allow them to delete that data. In compliance with GDPR, the process is done through Hilton's global privacy office," Manga said.

He added that across the layered architecture of a connected room, security is built in. "[Security] is a first-class citizen," he said.

While the hotel giant works to serve customers who want maintain privacy, it continues to experiment with technologies in ways that can improve the customer experience. One such example is robotic butlers, which are being tested in Hilton's labs, Magna said.

"These haven't seen the light of day -- but we are looking at how to make these types of technologies complimentary," Manga said. He added that AI has its place, but service industry workers get nervous about their job security when the topic comes up.

Hospitality IoT Checks In To Royal Park Hotel

By integrating smart hotel technology, one Michigan hotel hopes to revolutionise the guest experience, while optimising business processes.

By Sharon Shea, TechTarget

When guests arrive at their hotels after a long day of travel, they don't want to wait in line to check in. Thanks to hospitality IoT, this is a decidedly real scenario -- and one that's about to go into action at Royal Park Hotel.

The boutique accommodation, located in the Detroit suburb of Rochester, Mich., may have the English manor design of a historic landmark, but it contains some of the newest technologies available to offer its guests a comfortable and connected stay. Soon, guests will be able to go directly to their rooms, easily gain access and relax while reading the latest news, watching Netflix or catching up on email on their phone or tablet.

Improving Guest Experience

Improving the guest experience was the key driving force of the recent smart hotel technology upgrade, said Scott Rhodes, director of engineering at Royal Park Hotel. The 143-room hotel, which opened in 2004, partnered with Ruckus Wireless nearly a decade ago to install 30 Wi-Fi access points for its guests. 10 years later and with the growing use of mobile and smart devices, Rhodes knew upgrading the hotel's wireless bandwidth was critical. The property is now equipped with 160 Ruckus access points, one in each room, as well as others across the property. The access points installed under the desk in each guest room also contain an IoT module with a unique MAC (Media Access Control) address.

"Guests are coming in with two or three devices each, and if you have two guests per room, you have five or six devices," Rhodes said. "Being able to give them the platform with that reach and stability is a game changer." The improved bandwidth builds off Royal Park's existing Wi-Fi infrastructure.

"We use pretty much all the same infrastructure already deployed in a Wi-Fi network and add an IoT controller to manage IoT traffic," said Mark Grodzinsky, senior director and general manager of IoT at Ruckus Networks, now CommScope. The access points and the IoT controller, an on-premises virtual machine, are bundled into Ruckus' IoT Suite. The access points speak three languages—Wi-Fi, Zigbee and Bluetooth Low Energy (BLE)—and can accommodate nearly any IoT device or system.

Another benefit Royal Park will enjoy thanks to IoT Suite is an integration with smart locks. Seven years ago, Royal Park upgraded its Assa Abloy locks to a fob option, but Rhodes always knew there was something more to offer guests.

"We had the card insertion piece, then we went to the fob," he said. "And, at the time, I was really curious – you could see the opportunity on the horizon: the app for the phone." Yet, the technology just wasn't there yet. Six months ago, the opportunity to upgrade to smart locks arose.

"Now, after they make a reservation, the guest's phone or smart device can access their room once they hit the site in the period of time the reservation's good for," Rhodes said. Thanks to the connected locks, management can monitor when doors are open or closed, locked or unlocked. IoT Suite also includes what Rhodes called a "joiner piece" – if someone has a reservation in a guest room and is also renting a meeting room, the app will provide seamless access to both.

"It helps lessen the frustration," he said. "You're a meeting coordinator – you have a lot on your mind. You don't need to go down to the front desk to get another key."

Beyond convenience, the smart locks, which run on the Assa Abloy Visionline software system, provide increased

security for guests. If someone attempts to open a door lock with a device it is not associated with, the smart lock will notify management through a "wandering intruder" feature. The key on the wandering intruder's app will be null and void, and with mapping capabilities, the IoT system will alert management of the wandering intruder's location so security staff can investigate. Guests can rest easy if, for example, they leave their key or phone at the pool or lose it.

Hospitality IoT Benefits More Than Guests

Royal Park Hotel's IoT deployments—current and future—aren't just for guest convenience. A beta test of TraknProtect's safety buttons aims to improve staff and guest safety. BLE beacons installed on staff lanyards signal Ruckus IoT Suite when pushed, notifying management of the employee's exact location and a potential issue.

The safety alerts will also be instrumental in helping the hotel comply with an upcoming industry security regulation. "The hospitality industry, the unions, the brands – they've all been moving in the same direction," Grodzinsky said. "There was this 5-Star Promise that came from the [American Hotel & Lodging Association], where it said all properties in North America will have safety alerts in the hands of their staff by the end of 2020. It's a huge commitment, and this technology can be used to meet that promise."

Rhodes said the hotel also plans to complete a 90-day trial of IoT asset tracking, adding TraknProtect beacons to carts, trays and other hotel equipment, such as rollaway beds, used throughout the property. This will help manage inventory in storage, hallways and guest rooms, as well as notify staff when items, such as food carts or bed trays, should be picked up. A geofencing feature will also alert management when assets leave the property.

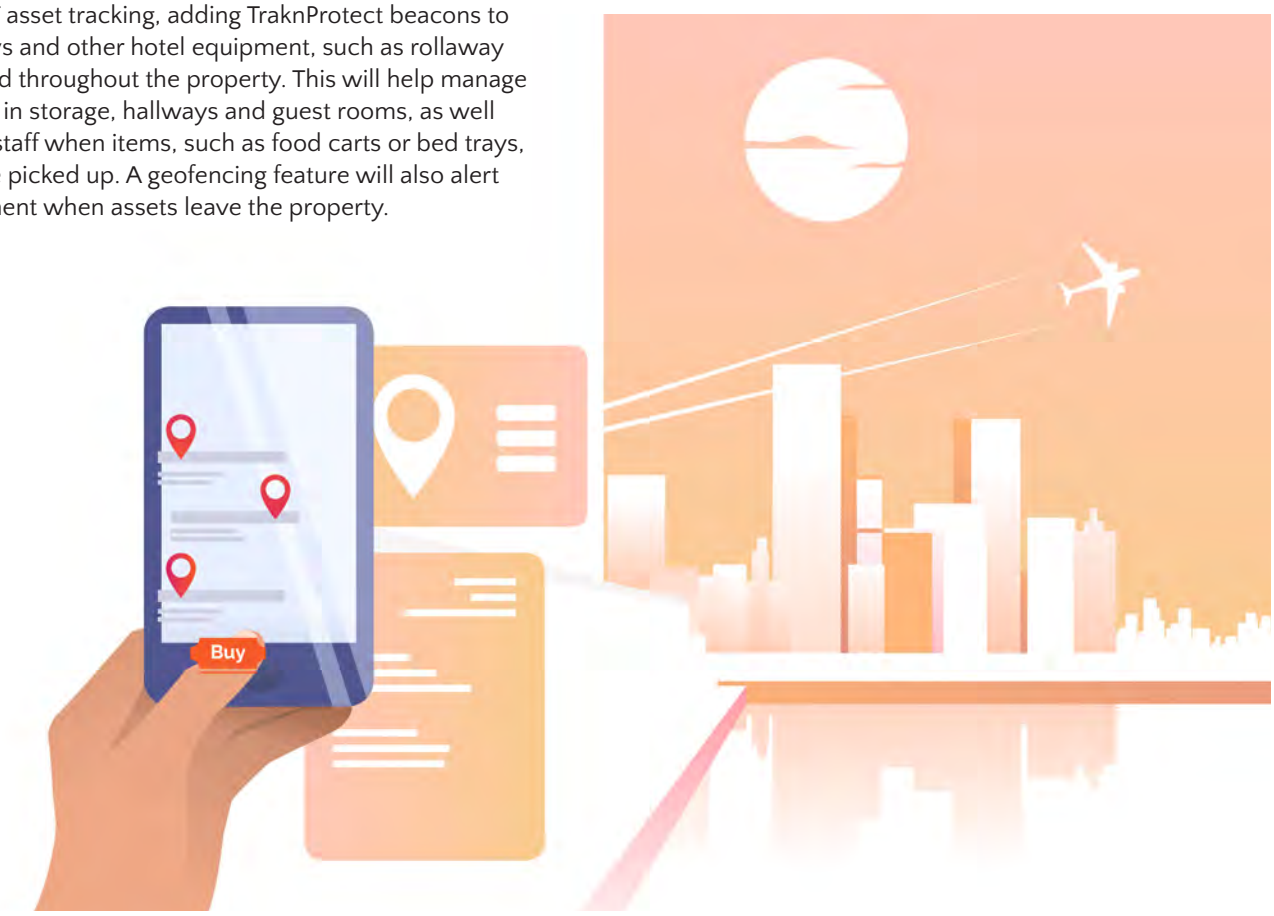
Down the line, Rhodes said he hopes to connect the hotel's lighting and HVAC (heating, ventilating and air conditioning) system through IoT Suite, adding smart thermometers to monitor room temperatures.

"In each of the rooms and across the property, you've got a deployment that has Wi-Fi, BLE and Zigbee, so you can connect other IoT devices to that same network, whether it be a TV or an HVAC system or lighting," Grodzinsky said. In-room automation, Grodzinsky said, is a major benefit of hospitality IoT and can help expand the guest's comfort and experience.

"The magic really happens not when you have any one thing individually connected, but when you consider what you can do now with the interactions," Grodzinsky said. "Say I open the door, which is a trigger event, and as I'm walking in, the drapes come up, the thermostat adjusts, the lights come on, the welcome screen happens on the TV – it's your welcoming event."

Smart hotel technology can also put the room to sleep when it detects there aren't any occupants.

"The ability to control [lights and HVAC systems], or just see what's going on in the rooms, lets you be a little more aware of your carbon footprint," Rhodes said, a potential source of major energy and cost savings in the hotel industry.



OUR WEBSITE HAS A FRESH NEW LOOK.

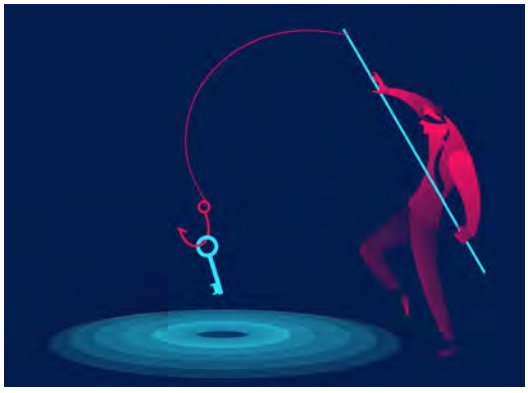
sst.tradelinkmedia.biz

Hospitality Industry At Highest Risk Of Phishing

Benchmarking report shows average phish-prone percentage across all industries and sizes of organisations at 29.6% – up 2.6% since 2018

By Warwick Ashford, Senior Analyst at Kuppinger Cole

Large organisations in the hospitality industry have the highest phish-prone percentage (PPP) of 48% and are therefore most likely to fall victim to a phishing attack, a report shows. On the other hand, the transportation industry is at the lowest risk, with large organisations in the sector scoring a PPP of just 16%, according to the latest Phishing by industry benchmarking report by security awareness training firm, KnowBe4.



However, the report shows that large organisations in the construction industry are the most phish-prone when examining both small and mid-sized organisations, with PPP scores of 38% and 37%, respectively.

Is Your Organisation Phish-prone?

The report is based on an analysis of nearly nine million users across 18,000 organisations with more than 20 million simulated phishing attacks across 19 industries. The PPP indicates what proportion of an organisation's employees is susceptible to social engineering or phishing scams. A high PPP indicates greater risk and a low PPP is optimal and indicates that particular workforce is security aware and able to recognise a phishing attack.

Among large organisations, energy and utility firms came in third place after hospitality and construction with a PPP of 34%.

In the medium-sized business category, the construction industry was revealed at the highest risk with a PPP of 37%, followed by insurance (35%) and manufacturing (34%). Among small business, construction again came top with a PPP of 38%, followed by retail (37%) and insurance (36%). According to the study, the average PPP across all industries and sizes of organisations was 29.6% – an increase of 2.6% on 2018.

Phishing – Top Threat Action

After 90 days of computer-based training and simulated phishing security testing, the overall PPP was cut in half across all industries. The PPP then dropped to just 2% after 12 months of security awareness training.

The report pointed out that, according to Verizon's 2019 Data breach investigation report, phishing was the top threat action used in successful breaches linked to social engineering and malware attacks.

These criminals evade an organisation's security controls by using phishing and social engineering tactics that often rely on employee naivete, the report said, with emails, phone calls and other outreach methods used to persuade staff to take steps that give criminals access to company data and funds.

Every organisation is at serious risk without new-school security awareness training, said the report. "With an average baseline PPP of 29.6%, companies could be exposed to social engineering and phishing scams by more than a quarter of their workforce," it said, adding that an effective security awareness training strategy can help to accelerate improvement, especially for large organisations.

Network Access Control: A Paramount For The Cybersecurity Industry

Organisations are facing a formidable challenge of deploying real-time automated threat response systems.

By Soumya Das, Editor at Progressive Markets

As organisations are increasingly focusing on interoperability and information sharing, IoT devices, virtual server / cloud services, routers, switches, firewalls, and bring-your-own-device (BYOD) are being flocked to their networks periodically. This poses a cumbersome task for network guardians to authenticate and authorise the endpoints in a network.

In the present scenario wherein users can access business networks from virtually any part of the world via various technologies and devices, network administrators have felt the need to transition from conventional solutions like antivirus, spywares, and firewalls that can handle tasks like simple onboarding and guest management to advanced technologies like network access

control (NAC) for attaining robust and dynamic role-based functionalities.

What Is Network Access Control?

Network access control, generally known as NAC, is a tool used for controlling and managing network access based on compliance with a network and its policies. These policies are devised based on various parameters like user identity, device location, device health, among others.

With the megatrends of IoT devices and BYOD reshaping the network perimeters and increasing the vulnerability of systems, NACs play a vital role in identifying and securing endpoints by knowing who, when, where, and how a device has connected to a network. Technically, NAC basically conducts a pre- and post-connection risk assessment of any access control device that attempts to connect to a network by using policies triggered by predefined protocols.

Evolution Of NAC

Earlier, NACs were based on the principle of authenticating and authorising endpoints through a simple scan-and-block mechanism. With technological advancements, providers are offering network access control solutions to address the burgeoning need to manage and restrict guest access to enterprise networks.

Adding to the complexity are factors like the growing prevalence of smartphones & mobile devices; unregulated BYOD policies; and advent of IoT, lack of device configuration standardisation for IoT and BYOD; possibility of myriad permutations of device type, brand, operating system, and security health status; and lack of enterprise grade security in the majority of devices that accentuate the complexity.

Thus, organisations have been opting for advanced NAC solutions that facilitate triage and quarantine functions in real-time without manual intervention.

Furthermore, the leap-frogging nature, intensity of security attacks, and growing need for scalability have augmented the demand for best-in-suite solutions to mitigate the risks of attacks and enable virtual as well as physical expansion in the future.

With massive proliferation of endpoints, NAC providers are developing advanced solutions. Security automation and orchestration solution (SA&O), agentless solutions capable of automated security orchestration, and others offer granular policies for both the user and the device, facilitate scalability, enable security orchestration and automation, and offer collation of security data at a central server for easy tracking.

Types Of Network Access Controls

Organisations across the globe have been leveraging NAC systems to detect and protect against rogue devices. However, selection of the right product is an arduous task which includes scrutinising network configuration compatibility, internal set up, and end users. Depending on the modus operandi of NACs, these systems are classified on the basis of characteristics and functionalities.

Based on design, NACs are of two types, i.e., pre-admission NAC and post-admission NAC. The former is based on the principle of inspecting end stations prior to being allowed on the network, while the latter is used for making enforcement decisions based on user actions after their entry into the network.

Another fundamental difference in NAC systems depends on the need to use agent software to report end system characteristics. Such systems continuously operate in the background of the device to monitor security compliance, and send updates to the policy server. The second, being a more advanced form, is the agentless NAC that does not require end point agents to authenticate and manage devices.

These systems ensure compliances at both endpoints before a user is granted access to the network. However, the major drawback of this system is that users are authorised by assessing the network traffic. This can make it easier for cyber criminals to gain unauthorised access to the network.

The third point of classification is based on the use of agents on end stations. Agent software is used on end systems to enforce policies, and report lapses to a central console

through switches. These types of NACs are known as out-of-band systems. In contrast, there are inline solutions or single box solutions, which secure the network by acting as an internal firewall in access layer networks, and enforce policies in case of an intrusion.

Depending on the need to deploy software or hardware appliances, NACs are categorised into hardware-based network access control and dynamic network access control. The former uses a device, which is preinstalled on the network, and operates in accordance with the network traffic.

The major limitation of this type is the periodic need to make changes in infrastructure and operational practices to permit defined access to end users. Moreover, the chances of failure are higher than other systems due to the constant changes in server configuration.

Alternately, dynamic NACs neither require software or hardware installations nor changes in the network configuration. It works on specific computers that are connected to a local area network, which are considered to be trusted systems. In case of an unauthorised user trying to gain entry into the network, the trusted systems would not grant access, and subsequently communicate the information to the main server.

Can A Legitimate User Be Denied Access?

NAC products are deployed to prevent some legitimate clients from gaining access to an enterprise network. This process is known as remediation. Thus, network access control solutions need a way to remediate such end-user problems that deny access. The two common ways of remediation include quarantine networks and captive portals.

A quarantine network provides routed access to only certain hosts and applications. It is implemented via VLAN assignment. A captive portal prevents HTTP access to web pages, and redirects users to a web application that provides instructions and tools for updating their computer. Until their computer passes the inspection, it cannot gain entry to the network, but would have access to the captive portal.

How Does NAC Work?

NAC system, when deployed, first creates an inventory of the devices connected to the network, categorises them based on attribute, and implements policies based on predefined rules created by the internal security team.

NAC products control the type and level of access to all the devices connected to the NAC network on a per NAC device basis, and also enable granular control for every action to ensure compliance with the internal policies. These controls are triggered by predefined policies configured in a central control system. Some policies are based on creating a whitelist of media access control (MAC) addresses, which makes it difficult for intruders to connect to the network.

The Cost Factor

NAC systems are available as either physical devices or VMware-based virtual appliances. The cost of these systems mainly depends on the number of endpoints required to be handled. However, on an average, these systems have an upfront cost of about $12,000–$30,000. Added to this, there are other support costs ranging around $2,500–$3,000 per annum, apart from the costs involved in imparting training to personnel for managing the product.

The true cost of deploying a network access control system also depend on other factors like installing add-on modules; support costs, including training; and staff time. Generally, NAC vendors centrally manage these systems using an NAC appliance or virtual machine. While, some vendors include training as a part of their package to demonstrate the features of the equipment, configuring policies, and alerting systems.

Conclusion

With security threats growing and changing at a frantic pace, and the daunting task of combating zero-day exploits, organisations are facing a formidable challenge of deploying real-time automated threat response systems. Advancements in NAC systems have assisted organisations to promote scalability and augment visibility, control, and response to the avalanche of threats and alerts.

With the burgeoning number of devices trying to gain access to networks and the plethora of security threats haunting enterprises, it is essential for them to deploy solutions that are robust and provide dynamic role-based permissions for easily and automatically accommodating users and devices to the network as the same time maintaining NAC security.

Nevertheless, organisations need to understand that NAC is not a silver bullet that can protect their network against all types of threats, rather it should be used along with other systems, such as intrusion prevention system (IPS), mobile device management (MDM), next-generation firewall (NGFW), security information and event management (SIEM), and threat detection software to ensure complete network access protection.

On the global scale, the NAC market is catered by two key players, viz. ForeScout Technologies and Cisco Systems, Inc. The other providers in the sector include Microsoft, Auconet Inc., Avaya Inc., Bradford Networks, Extreme Networks Inc., Hewlett Packard Enterprise Development LP, Impulse Point, Key Innovator, Portnofx, and Pulse Secure, LLC.

Zero Trust – The Modern Approach To Securing The "Keys To The Kingdom"

Identities are an organisation's most significant vulnerability. Trust no one, verify everyone.

By Daniel Mountstephen, Regional Vice President of Centrify Asia Pacific & Japan

Remember Kevin – the kid from "Home Alone"? After waking up to find that his family had left him behind, he saw two burglars trying to break into his home. Despite his commendable efforts to secure his house from these intruders, there came a point where he had to face facts – they're going to get in. That's when he really pulled out all the stops – scattering Christmas ornaments on the floor, tarring the basement stairs. Essentially, doing all he can to keep what's valued, safe.

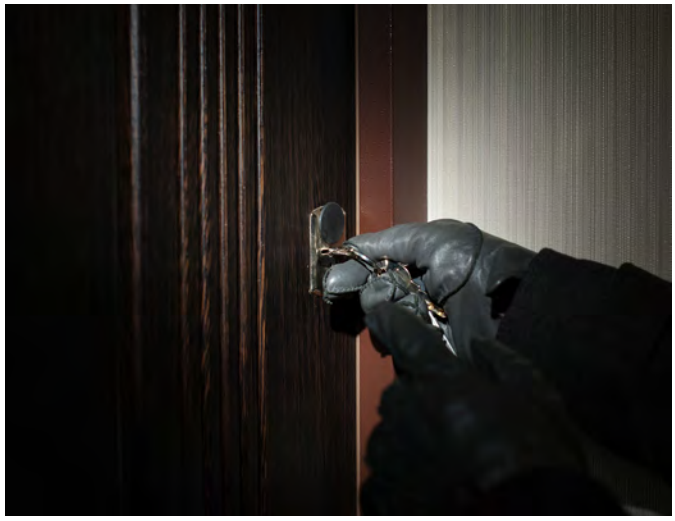
Now, think about this for your own organisation's network – how well protected is it? Are perimeter protections really enough? Or are unauthorised users already in the network?

Organisations today should take the same mindset – to trust no one, assume the intruders are already in the network, and create a series of challenges to limit movements and keep them from the most critical systems and data. Just like the burglars' will to break into Kevin's house, Mobility, cloud, IoT, and social media are today's muse for intruders to access an organisation's network. With each new attack surface comes the opportunity to leverage trusted identities without proper access controls.

Despite spending billions on cybersecurity and risk management, organisations are losing the fight to protect sensitive information. Employees, partners, contractors, and customers can connect anytime, anywhere from any device to any resource. These freedoms make their identities prime targets for criminal hackers, who have wasted no time using them to raid accounts and data.

Identity Is The Primary Attack Vector

In 2018, the SingHealth data breach saw 1.5 million patients' personal particulars and another 160,000 outpatient medication records illegally accessed by a hacker who was able to stay within the network for months, without detection.



More recently, Sephora Southeast Asia was responsible for the leakage of 3.2 million customer records. What was most alarming was the fact that no major vulnerability was found on Sephora's website, and no cyberattack could actually be traced.

Criminal hackers tie 70% of their breaches to user activity, according to Forrester. In a survey conducted by the leading Privileged Access Management vendor Centrify, and the Dow Jones Customer Intelligence team, 62% of CEOs inaccurately cite malware as the primary threat to cybersecurity, yet only 8% of all executives said that anti-malware endpoint security would have prevented the "significant breaches with serious consequences" that they experienced.

An AT Kearney survey last year emphasised that organisations in the ASEAN region must secure a sustained commitment to address its cybersecurity gap and build the next wave of cybersecurity capability. Compared to the global average spending on cybersecurity of 0.13% (as percent of GDP), the ASEAN region invests just 0.06% of its combined GDP on cybersecurity.

The region's expanding digitalisation only makes it an even greater target. According to a survey by a global professional services firm Marsh and McLennan, organisations in Asia are 80% more likely to be cyberattacked.

Bottomline: Something must change. Today's security is not secure.

The New Reality: Never Trust, Always Verify

Cyber-attackers today are looking for the easiest way in. So, they no longer "hack" in – they log in using our own weak, default, stolen or otherwise compromised credentials against the organisation. Identities can slip from good to bad at any point.

With the explosion of new attack surfaces and unwieldy identities, the old cybersecurity adage of "trust but verify" no longer applies. The new mandate is "never trust, always verify" – a Zero Trust approach is paramount for all organisations today.

Credentials, especially those for administrators with privileged access to critical systems, are the keys to your kingdom and your most significant vulnerability. Perimeter security is not enough to protect today's world. It would be like continuing to invest in the moat when the castle of the kingdom no longer exists.

Centrify is redefining the legacy approach to Privileged Access Management by delivering cloud-ready Zero Trust Privilege to secure modern enterprise attack surfaces. Centrify Zero Trust Privilege helps customers grant least privilege access based on verifying who is requesting access, the context of the request, and the risk of the access environment. By implementing least privilege access, Centrify minimises the attack surface, improves audit and compliance visibility, and reduces risk, complexity and costs for the modern, hybrid enterprise.

Over half of the Fortune 100, the world's largest financial institutions, intelligence agencies, and critical infrastructure companies, all trust Centrify to stop the leading cause of breaches – privileged credential abuse.

A Path To More Secure Access Control

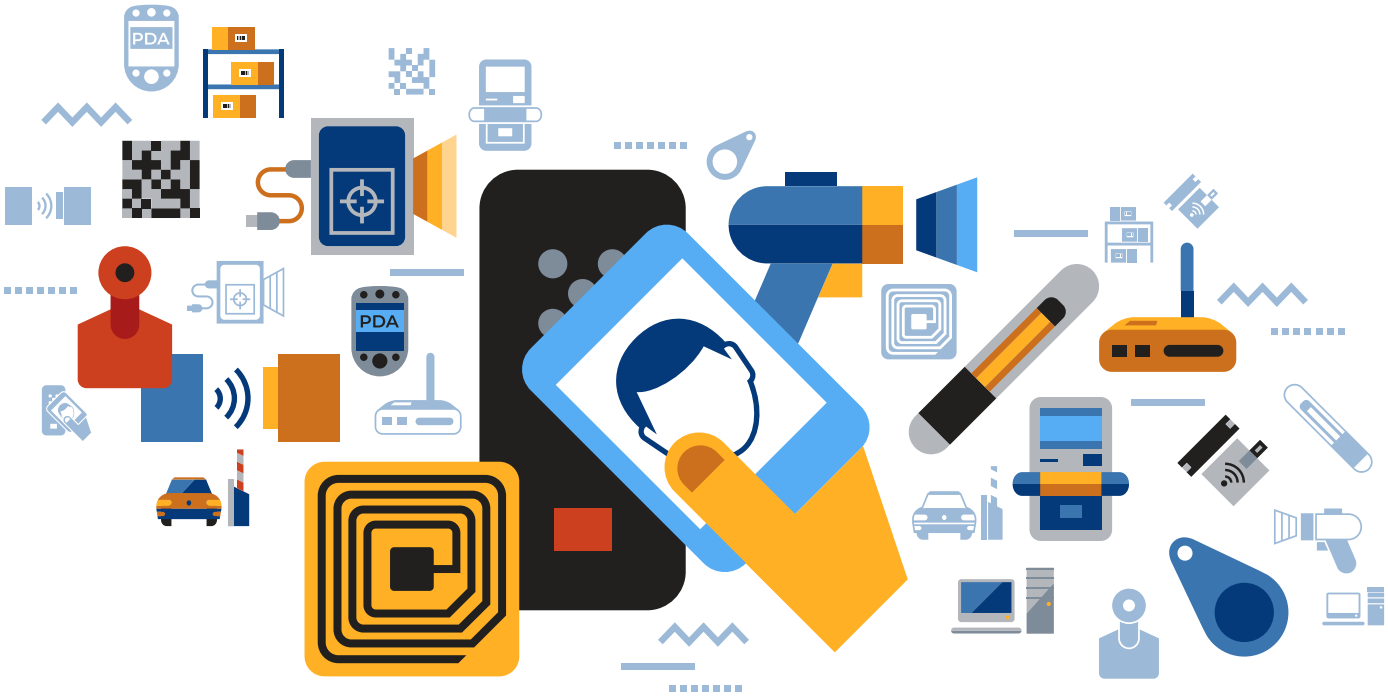
In the past, when organisations chose RFID for controlling access, they were motivated most often by reliability, Cost, and user convenience, regardless of whether they intended their solution for pedestrians or vehicles. By today, RFID's benefits over traditional locks and even magstripe have become familiar and have been accepted for decades.

Reproduced from White Paper by Idesco

Regardless of a system's technology, most permit extremely convenient adding and removing of users, usually with little more than a couple of mouse clicks. The savings RFID offers over the costs to replace traditional locks when keys are lost is merely one of RFID's strongest selling points.

After RFID's appearance, the public came to assume—wrongly—that all its technologies possessed roughly the same data capacity, flexibility and security. Nothing could be further from the truth today. RFID technologies differ greatly, even profoundly. This makes it vital that any organisation considering RFID first learn about its technology differences.

In particular, the different security features offered by access control technologies have become the central factor to consider when planning to deploy RFID. For, as you will discover here, the technology you choose will be foundational to your site's security, particularly its asset and personnel protection, for an interval that could last decades.



The first RFID access control technologies relied on reading short, but unique serial numbers (or UIDs) encoded in user transponders. It was a logical, simple solution that allowed data to be collected while access was controlled. Transponder security was literally a negligible concern despite transponders being readable by any suitable device. Why? Because readers and their underlying technology were not commonplace or prevalent. At that time, quite simply, no one worried about their transponders being cloned.

Returning to the present, things have changed – a lot. Devices designed explicitly to clone transponders or skim transactions of unsuspecting users are now readily found in web shops and advertised in hacking blogs. Meanwhile, YouTube now hosts numerous "how to" videos offering detailed instruction to would-be hackers. It is now essential that security managers and system integrators alike carefully weigh hacking risks against a site's security needs if it utilises an older, legacy technology. Far too frequently, ill-informed sites expanding or replacing readers have opted to retain legacy technologies, considering only the costs and inconvenience of migrating while seemingly oblivious of the growing risk.

As a result, for sites still using older or UID-based technology, a new imperative has appeared: migrate to greater security before property loss, damage, or worse, user security is compromised. And, regardless of the solutions considered, a final migration choice must be based on careful risk analysis and technology comparison rather than simply settling with something familiar. It deserves mentioning that risk managers for the most security-sensitive sites today invariably demand secure, unhacked access control technologies to ensure levels of indemnification their insurers would otherwise not underwrite.

With that as a preface, don't allow the convenience of familiar risks to lull you into dangerous complacency; the assumption that security improvements are necessarily time-consuming or even costly can put your organisation at even greater risk.

Pin Codes

System integrators almost universally agree: the most cost-efficient way to meaningfully enhance access security at a site still using UID transponders, is to implement user-specific pin codes at access. The logic is simple: if a skimmer/hacker clones the UID of a user transponder they will still be denied access without the correct corresponding pin when they attempt entry with their cloned transponder.

Admittedly, a hacker could theoretically survey the original user of their cloned transponder when they enter their personal pin code. However, their success will unavoidably demand a much higher threshold of resourcing, commitment—and potential risk—than mere UID transponder cloning. How much higher a threshold is arguable.

For example, vacation property managers, issuing transponders to a constantly shifting population of users have rightly argued that pin codes make no difference. By contrast, a site manager issuing transponders to permanent employees might judge a new pin protocol satisfactorily augments his site's property security. In the end, the point of user-specific pin codes is to increase the burden of resourcing, commitment and endured risk on hackers to defeat it. Not surprisingly, some security managers opt to complement pin codes by deploying comparatively

inexpensive recording video systems to deter hackers from attempting to survey pin code entries from even discreet distances.

Nevertheless, adding user-specific pin codes means choosing a reader more carefully if it will be sited outdoors. Why? Because some manufacturers overlook how inclement weather, and particularly cold, snowy or icy conditions renders mechanical keypads inoperable. Rainwater or condensation clinging to the back of a key can freeze between it and its actuator, or snow crystals can become lodged there by wind or by users attempting to brush away snow.

As a Scandinavian manufacturer, Idesco instantly foresaw this problem and committed to designing for it. We designed keypads that lacked moving parts to be clogged by snow or ice. Instead we opted on capacitive switching to register code entries. More recently, Idesco began offering mechanical keypads that possess the same IP67 protection ratings as their predecessors. These new keypads use compression-moulded switching to detect key depression, providing valuable, convenient tactile feedback during pin code entry, yet still preserving the very robust IP67 protection rating of earlier Idesco keypad models.

Despite the enhanced security pin codes provide, a responsible security or site manager must be able to recognise when it will be insufficient to protecting their site. We turn now to measures designed to meet higher security thresholds.

Securing Your Entire Network

OSDP (Open Supervised Device Protocol) is a standard that America's Security Industry Association (SIA) released in 2012. SIA had organised and defined OSDP to give the access control industry a regularising standard to follow in defining bi-directional data transmission between readers and hosts (controllers and/or systems). OSDP also chose a slightly more advanced cable than RS-232 or Wiegand: RS-485. RS-485, in addition to supporting bi-directional data transmission, also transmits much greater amounts of data than Wiegand – and over much longer distances.

SIA also defined OSDP as an open standard to ensure seamless interoperability between compliant devices, even when they are sourced from different suppliers. OSDP's latest iteration, v2 (2.1.7), has been enhanced to also powerfully protect its data stream with effectively unbreakable 128-bit AES encryption. Each session deploys a unique, randomly-generated encrypting key. This defeats hackers who might attempt 'replay attacks' (e.g. recording transactions then re-playing them later to spoof the controller into opening a door).

OSDP's most important security feature is its ability to encrypt the data stream between readers and controllers. This encryption in OSDP's latest version (v2), gives data effectively impenetrable protection from even the most sophisticated skimming efforts, whether attackers try to skim the air interface of transponder reader transactions, skim amplitude fluctuations emanating from readers' cable interfaces, or attempt a differential extraction using both.

In addition to the constant random key cycling that secures each OSDP v2 session, skimmers are also stymied by the EM noise generated by RS-485's bi-directional data flow, which catastrophically contaminates attempts to eavesdrop on an OSDP network.

In addition to these daunting security features, however, OSDP v2 also provides an attractive convenience for users, site managers and integrators. Its highly secured sessions may now also be used to safely forward confidential, personalised messages to transacting users wherever their readers possess a display.

Designed by macrovector / Freepik

Smartphone Access Accelerating The Transition Away From Cards And Fobs

Mobile access technology enables other use cases that aren't possible with today's keycards.

By Kellen Duke, Head of Deployments and Security with Proxy

When you enter the lobby of the recently opened Salesforce Tower in San Francisco, the tallest building west of the Mississippi River, things look a little different from the typical commercial property. Tenants and visitors breeze through the turnstiles, swiping smartphones to gain access. At elevator dispatches, people tap their phones to call an elevator to their floor. And upstairs, people seamlessly access secure doors using their mobile devices. If this scene is any indication, it's time to plan for the advancing tide of smartphone access technologies.

What's Driving Smartphone Access Adoption

The iPhone was released 12 years ago this summer and Bluetooth-enabled phones have been around even longer. But it's only recently that this technology has matured enough to use in mission-critical physical security applications. Today, the technology is ready, and adoption is accelerating due to the confluence of three interconnected trends.

First, enterprises and property owners are looking to make access control easier to manage. The average company loses 2.6 cards/fobs for every 10 employees every year. Moving to mobile access significantly reduces the manual effort of security personnel to respond to a loss incident. Employees are also far less likely to lose their phone, which they own, and report the loss sooner and that reduces the risk of someone gaining access with a stolen phone.

Another key driver of smartphone access is that it offers a better end user experience. One of the primary complaints office workers have about access cards (45.4% of people surveyed) is that you always must carry it with you, or that they need to carry more than one card because they visit multiple office locations that use different access technology. Mobile access consolidates multiple cards into an electronic wallet that lives on the device so there's no reason to fumble with multiple plastic cards again.

Because access cards live electronically on the device, it's no longer necessary to physically deliver a card or badge to someone to give them access. That can have a big impact on the experience of visitors to the office. Previously, visitors have had to wait in line at the security desk in the lobby to sign in and receive a temporary badge or QR code to go upstairs. Now, hosts can send their visitors a temporary access card directly to their phone. When the visitor arrives, they simply tap their phone to access the turnstile and meet their host upstairs on their floor.

Finally, and this shouldn't come as too much of a surprise, the encryption and tokenisation capabilities of software running on the supercomputers people carry in their pockets trumps RFID cards. Many card formats can be easily cloned and others that are more secure are cost prohibitive, especially when you consider how frequently employees lose cards. Smartphone access technology makes it more challenging to execute a replay attack to gain access. And the technology opens novel new security options like biometric authentication using the facial recognition or fingerprint recognition technology on many smartphones today that can ensure the user holding the device is in fact the person who has access to the building.

Balancing Data Accessibility With Security Controls

How can infosec pros and data architects work together to support business goals and achieve a good level of cyber security?

By Simon Persin, Director at Turnkey Consulting

Data architects and infosecurity professionals might work for the same organisation and spend much of their time dealing with data, but that is often where the similarities end. While data architects focus on how data can flow smoothly and quickly through the organisation, security professionals are tasked with containing data as much as possible so that it doesn't fall into the wrong hands. In other words, the two professions live in competing worlds.

But as a growing number of enterprises realise that data is key to their success, we need to look for ways for these two "sides" to align their objectives and strengthen their working relationship. This calls for a balance between access to data being granted only to those who need to view it, and making sure data is always available where and when it is required to allow the organisation to function.

This isn't as big an ask as it may first appear. At their core, both groups recognise that data integrity is fundamental, which means keeping confidential data confidential. The domains may compete, but they run parallel to each other, rather than in opposite directions.

Core Challenges

But there are challenges. Cyber security teams often focus on the macro and micro levels, looking at specific fields, such as how individual files are accessed and how this access will be granted. At the other end of the spectrum, data architects often work at the conceptual level, or on data models that assume an ideal of free information flow.

Areas of conflict include infosec professionals objecting to data being combined and publicly accessed, or finding that users have stored duplicate copies outside centralised business intelligence tools, while data architects often don't want to deal with network segregation.

Problems are exacerbated by the lack of interaction between the two groups. In some organisations, this occurs only if security wants details of what data is present within a data object, or when the architects need confirmation that they can store more data in yet another cloud provider.

Finding Common Ground

Key to working together better is for each side to comprehend both the concerns of the other group and their context, and for this knowledge to be used to work out what can be done to avoid
that friction.

For architects, this means understanding an organisation's classification schema and what constitutes sensitive, or privileged, data. From there, they can be more selective in what data is extracted from systems and databases, and be conscious of creating privacy or data sensitivity issues if combining two (or more) sets of data reveals more information than intended.

For example, a list of factories exported from one source is fairly anodyne, but used in conjunction with separately sourced information on hazardous products and shipping details potentially flags where these materials are stored and puts the enterprise at risk.

Security, on the other hand, needs to apply appropriate controls based on the data present and the way it is accessed, rather than adhering to an inflexible set of policies and standards. Controls should reflect the way the business works and protect the data requester from causing an accidental data breach, rather than forcing onerous controls that employees will bypass if they prevent them from getting on with their job.

Communication is key to fostering this shared understanding and this can be reinforced by specific actions in a project delivery framework, such as a data privacy impact assessment during high-level design or a data sensitivity check once the solution has been built. However, the aim is to get people working collaboratively and in a more continuous manner. This is achieved more easily via good personal working relationships and when each team has empathy with the other's pain points.

We are moving further and further into an age where even the smallest organisations are collecting more data per second than they have in the past 10 years. This makes it critical that architects understand what they are collecting, why they are collecting it, and where it is being stored, while security needs to recognise that not everything needs to be protected to the same level, or in the same way.

Organisations are looking at a future where having thousands of data points is the norm, from smart offices controlling the lighting, to devices in the field collecting telemetry. Volumes will be such that a company cannot possibly store and organise it all, nor can security expect to protect everything. Rules will need to be set to decide what should be retained (the key elements for reporting) and what can be discarded.

As data combines and manipulates itself into thousands of different forms within seconds of being processed, applying a hard-and-fast classification schema will not be possible. New tools and ways of working need to be developed to identify the "sensitive" elements within a data flow (a person's name, or a bit of intellectual property, for example) so that the relevant policies are applied only to this subsection. This will improve the efficiency of any controls, rather than treating an entire data source as one item and applying the same level of control to everything, regardless of the need.

Similarly, as more data is collected from multiple sources and combined, the inadvertent creation of privacy issues needs to be considered. It is one thing to collect telemetry from a company vehicle, but if the business intelligence (BI) data lake then combines that with the HR department's list of drivers, and a list of who is driving which vehicle, then suddenly we are tracking individuals on a new level, which goes against most companies' privacy policies.

Viewed in these terms, it is clear why it is not an option to keep the worlds of infosec professionals and data architects separate and unconnected.

Cloud-Native Environments: A Challenge For Traditional Cybersecurity Practices

The Cloud is just a marketing buzzword that hides tens of thousands of racks in data centres filled with servers. In this context, security responsibilities remain very concrete but need to be approached and organised differently.

By JC Gaillard, Founder and Managing Director of Corix Partners

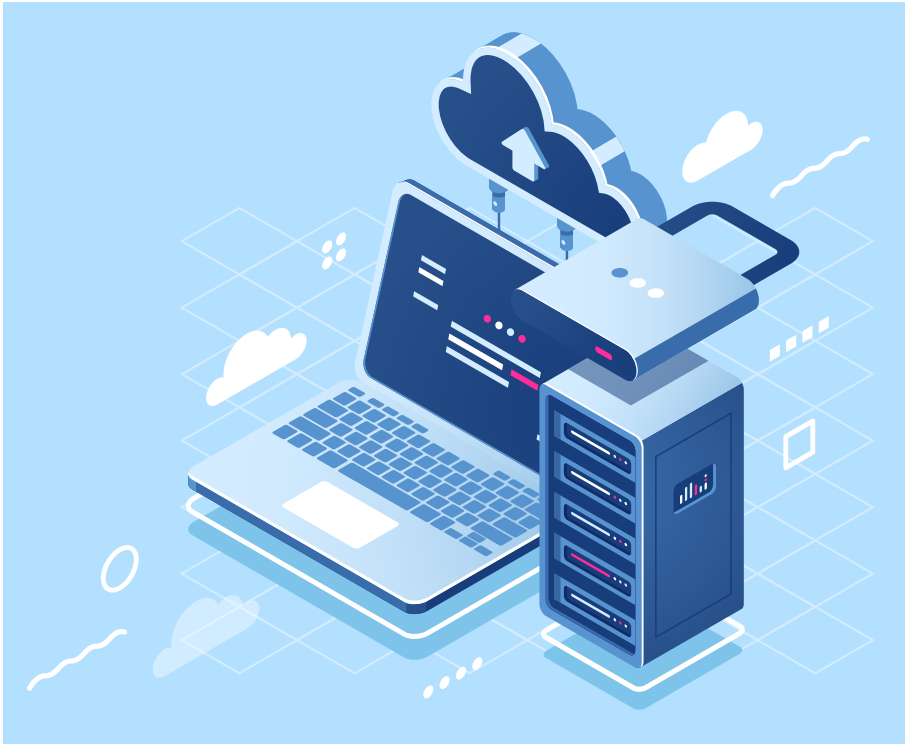
From the early days of computing and through the first phase of the Internet explosion up to the early 2010s, companies were mostly protecting their information internally, and they usually had some form of direct control over it. Most security standards and accepted good practices were drafted in that era and are still heavily inspired by a world where you could know where your data and your servers were.

In recent years, however, the development of massive computing and storing capacities in the hand of a few internet juggernauts led to the rise of the cloud economy. For the last decade, companies of all sizes—from tech start-ups to Netflix serving in excess of one hundred million users globally—have been moving their mission-critical servers and operations to the data centres of Google, Amazon, or Microsoft.

Infrastructure As A Service (IaaS)

On the face of it, the development of Infrastructure as a Service (IaaS) should be good news for the state of cybersecurity. Economies of scale and their vast pool of talents should allow tech giants to dedicate more resources into properly securing data centres. Servers should be easier to patch in a timely manner; state-of-the-art firewalls should be used and the physical location of these data centres should be heavily guarded.

In this context, it's easy to believe that moving to the cloud could mean solving many of your cybersecurity issues. It's also easy to believe that moving to the cloud would make your cybersecurity someone else's problem. Nothing could be further from the truth. Of course, each



Designed by fullvector / Freepik

organisation retains its own regulatory obligations irrespective of how operations are technically delivered.

For example, going to the cloud will not make any business GDPR-compliant in and of itself. In fact, all of GDPR's most important prerogatives around cybersecurity—adequacy of the protective measures, appropriate data management processes around consent, retention and deletion, etc.—do remain firmly within the organisation's remit. Not only is the Chief Information Security Officer (CISO) still a cornerstone of your GDPR strategy, but it inherits a new key role: that of dealing and interacting with Cloud vendors in this new world where your physical technology stack is delegated to someone else while the regulatory obligations remain firmly in your hands.

Looking at Amazon Web Services' Shared Responsibility Model makes this dichotomy very clear. Amazon Web Services (AWS) is responsible for the security "of" the cloud while you remain responsible for the security "in" the cloud – atop of which sits your consumer's data. While a car manufacturer is responsible for the security of your car, you're ultimately responsible for driving safely.

Similarly, AWS will never prevent you from driving into a tree. In their own words: "AWS trains AWS employees, but a customer must train their own employees."

The Cybersecurity Challenges Of Platform as a Service (PaaS) And Hybrid SaS Models

Platform as a Service (PaaS), Software as a Service (SaaS) and all hybrid models, of course, bring up the same challenges, often compounded by their inter-dependence (e.g. a SaaS solution built on IaaS or PaaS services), and a real supply chain which can become blurred very quickly.

The issue brought by the shift to the cloud paradigm in cybersecurity isn't one of adaptability but of adaptation. As such, a key role for the CISO is increasingly to act as a bridge between internal structures and cloud suppliers in order to ensure that all stakeholders are aware of all security requirements (driven by internal policies or regulation) and that all appropriate measures are in place.

This evolution in the role of the CISO epitomises a fundamental trend in cybersecurity which centres more and more activities around governance, people and culture rather than technology, data and networks.

Back To "Trust But Verify"?

It does challenge organisational models as well as the profile of the CISO, and brings to the forefront vendor risk management practices: in the cloud, you're never sure of what's really going on; your relationship with vendors is framed by contracts which are often one-sided, and a small SaaS provider carrying out sensitive business operations could expose your organisation considerably.

For regulated industries (which isn't in the age of GDPR?), blind trust will never be enough, and being able to demonstrate a sufficient degree of due diligence on key vendors will always be essential to defend against any liability in case of a data breach.

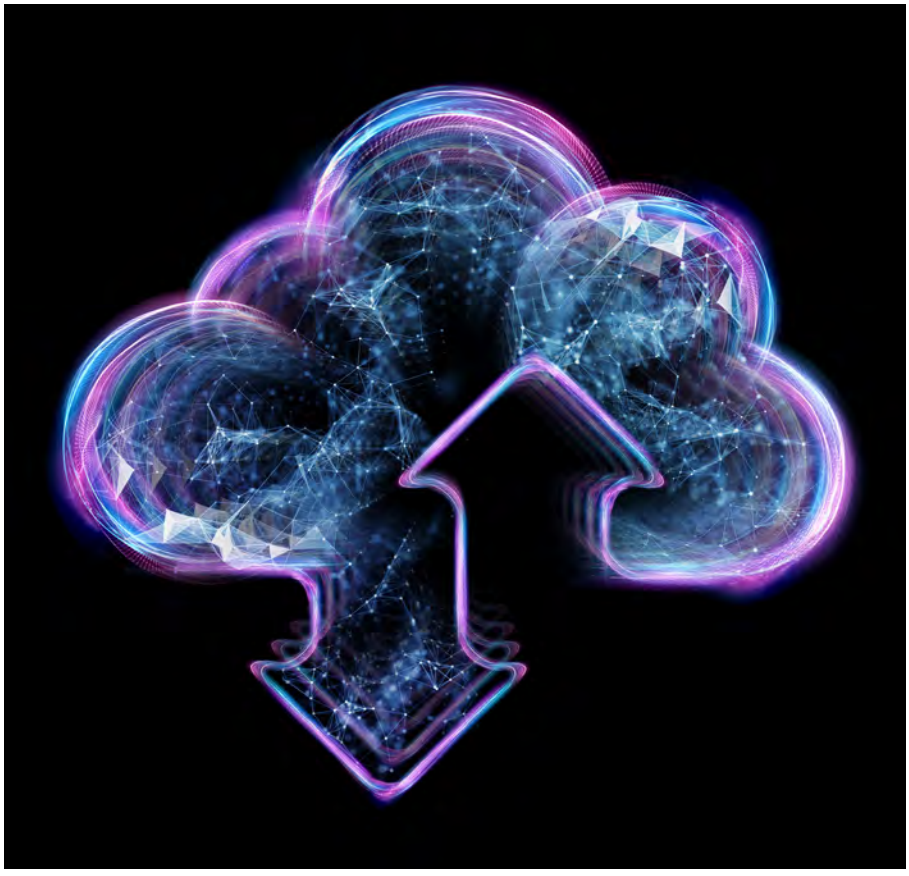
It's Time To Get Real: Exposing The Top 10 Cloud Security Myths

Despite the accelerated pace of cloud computing adoption, concerns about security show few signs of going away. In fact, security concerns actually grew among cybersecurity professionals in 2018 – reversing a multi-year downward trend.

By AL Perlman, Security Round TablePartners

According to the 2018 Cloud Security Report, nine out of 10 cybersecurity professionals now say they are concerned about cloud security, an increase of 11% from the prior year's survey.

If cybersecurity professionals are increasingly concerned, what does that mean for board members and other business leaders? It means it's time to get smart about cloud cybersecurity so you know what questions to ask the pros and what issues to stay on top of. In today's environment, what you don't know can hurt you. Not only that, you can also get burned when you think you know something that is not necessarily accurate.



We spent time chatting with Tim Prendergast, Chief Cloud Officer, and Sean Duca, Vice President & Chief Security Officer for Asia Pacific at Palo Alto Networks. Together they helped us to identify—and expose—10 of the biggest security myths about cloud computing and security. So, without further ado:

Myth No. 1: Cloud Is Less Expensive

Many business leaders are sold on the promise that cloud is less expensive than on-premises infrastructure. Yet, when it comes down reality, they typically find that their organisations actually wind up spending more. "It's not cheaper because they are not taking advantage of the cloud's elasticity, because they don't have the proper governance in place, and are not taking the time to work on it and make it cheaper," Prendergast says.

Duca says organisations must develop an understanding of what

the cloud can offer, and what it can't. "Most organisations are not getting the efficiencies they need," he says. "They are experiencing cloud sprawl and are starting to pull back." It takes knowledge, experience and commitment, Prendergast and Duca say, to explode the myth that cloud is less expensive and, instead, turn it into a reality.

Myth No. 2: Public Cloud Is Not Secure

The business model of the public cloud providers is wholly dependent on security. They have invested many millions of dollars in security, have the most up-to-date technologies, most sophisticated secure operations centres, use shared threat intelligence, regional data centres—the works.

"Nowadays a public cloud provider has world-leading security in every major geopolitical zone," Prendergast says. The problem for many organisations is they don't understand the cloud's shared-responsibility model. "Business and security leaders are afraid of losing control," Duca says. "They can't see it, touch, so they think they don't have control. If they don't understand the shared-responsibility model, they don't understand what type of security is available to them.

Myth No. 3: Public Cloud Secures Everything

This is the flip side of the shared-responsibility model. "Well," the myth goes, "if I trust the cloud to be secure, once I set up my cloud, I'm done." The catch, of course, is that the public cloud provider is only responsible for securing their infrastructure—you are responsible for securing your data and applications stored in that infrastructure.

Prendergast likens cloud security to home security. "You have a house with doors, windows, perhaps an alarm. You have the tools, but you still have to lock the doors, close the windows, set the alarm. You have to practice good cybersecurity hygiene. The cloud is no more secure than you make it."

Myth No. 4: We Can't Move To The Cloud For Security, Compliance, Data Sovereignty Or Other Reasons

Any cybersecurity or business leader who says his or her organisation can't use public cloud because of security or data privacy risks, is probably already deeply immersed in public cloud with some of their most important data and applications, Prendergast says.

"Every time we talk to a company and they say their data is too important to put in the cloud, we ask them what they are using for HR or customer relationship management," he says. "Invariably the answer is either Workday or Salesforce.com or both. We ask if they are using Office 365 or other software-as-a-service applications. They say, 'Yes.' We explain that their most critical customer and personnel is already in the public cloud."

Myth No. 5: Once We're Set Up In The Cloud, We're Done

Wouldn't it be nice, says Prendergast, to live in a world of no new vulnerabilities? "If nothing ever changes, no one new ever logs in again, yes, you're done. In the real world, the cloud requires ongoing care and feeding just like every other IT environment."

Duca says business and IT leaders need a "cloud security mindset." Cloud usage does not remain static. "You need to evolve. Cloud providers are making changes, and you will be making changes to your own software, who will be accessing data, etc. The threat environment changes too. One of the most common vulnerabilities is that people get complacent. What you may think is secure today, could change the very next day."

Myth No. 6: Compliance Is More Complex In The Cloud

Actually, one of the reasons to use public cloud is because meeting compliance and data sovereignty requirements can be a lot less complex. "Cloud providers have more tools and capabilities to check and measure what is going on," Duca says. "With data sovereignty, they let you keep data in a particular region. It is typically easier to ensure this in the cloud than with internal networks, where data and applications can be all over the place."

Prendergast says public cloud providers have cone a really good job of meeting frameworks for underlying compliance requirements. "You can inherit a lot of those controls," he says. "Cloud is programmatic, so if you take proper advantage of what is available, you can use scripts and software to manage compliance all year long. It's important to understand you have to work on it continually, so that compliance is continuance."

Myth No. 7: Cloud Security Is Managed The Same As On-Premises Security

"With public cloud, you don't have a lot of the physical infrastructure you would normally have—setting up racks of servers, running cables, power, etc.," says Prendergast. "It's like walking into a data centre where one day you had 500 servers and the next day you have 10. It looks like you were robbed. That's just a normal day in the cloud. If the data centre is hit by a distributed denial of service (DDoS) attack, it's hard to add 100 physical servers. In the cloud, you just click a button and scale up to 1,000 servers and make the DDoS inert and just pay for the day. You can scale up in just two minutes."

Myth No. 8: Everything Is Exposed On The Internet

Once again, we return to the reality of a shared security model, not the myth that your data and applications will automatically be exposed on the internet. "What you expose is up to you," Duca says. "It's your own perimeter. You can leverage the cloud to just host your apps and not put data there."

Prendergast says this myth may come from the word "public" in public cloud. "Public means anyone can use it, not that your data is public," he says. "The only thing exposed is what you want to have exposed. You have options to use virtual private networks, virtual private clouds, servers with no internet access. You are in full control, it's all a matter of how you set up and manage that control."

Myth No. 9: You Can't Innovate Quickly Because Security Will Always Lag

This is a myth that may have been perpetrated by a dynamic in which DevOps teams turned to public cloud because they couldn't afford to wait for legacy purchasing and deployment processes. This accelerated time to market, but it also may have introduced security gaps. It doesn't have to be this way anymore. "We've seen with DevSecOps that security should be part of teams, embedded in development approaches, whether in cloud or on-premises," Prendergast says. "They key is to treat security as a feature. The myth is that you can't do rapid development and security in the cloud. The reality is that cloud is actually an enabling technology for DevSecOps."

Duca says cloud easily supports DevOps advances such as containerisation and microservices. "You can decouple the development of code, push changes out, manage change processes through agile development. All of this can accelerate innovation, time-to-value and quality control."

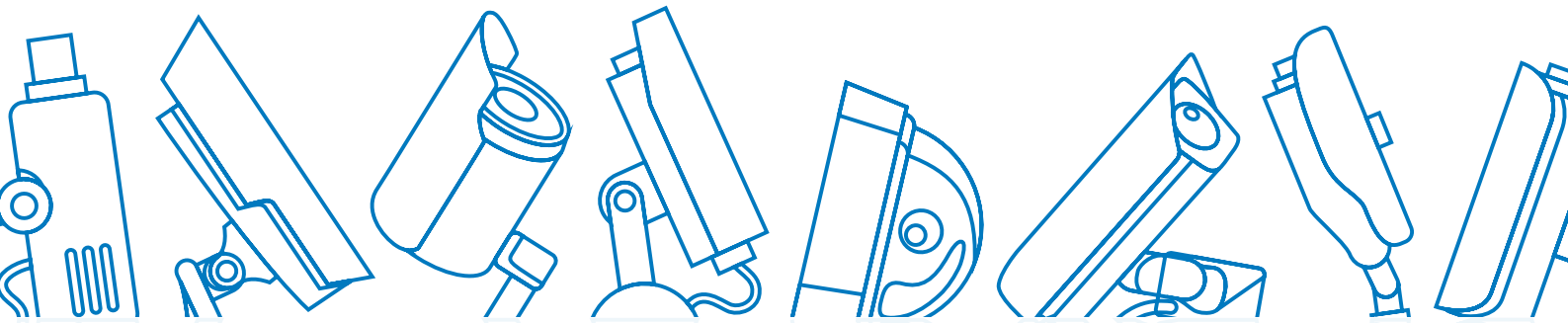
Myth No. 10: You Need A New Team For Cloud Security

The survey from Cybersecurity Insiders asked respondents to identify their main barriers in migrating to cloud-based security solutions. By far their main barrier was "staff expertise and training," cited by 56% of respondents. Next were data privacy at 41% and lack of integration with on-premises security at 37%.

The myth is that the same people who have built and managed your on-premises data centres can't adjust to the cloud era. This doesn't give them enough credit, Prendergast says. "What we've always seen is that many IT people are excited and challenged by technology advancements," he says. "Cloud is the new thing and many of your best people will make the transition naturally. You don't have to replace them; you have to encourage and support them."

Conclusion

When it comes to the cloud, the opportunities for business benefits are too powerful to ignore—agility, cost savings, time-to value and digital transformation, to name few. The security issues are also too powerful to ignore, which is why your teams must be focused on the real issues, and not the myths. When it comes to cloud security, it's time to get real.



SECURITY SOLUTIONS TODAY

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

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

Scan to visit our website

WE ALSO PUBLISH

bathroom+kitchen today

SEAB SOUTHEAST ASIA BUILDING

SOUTHEAST·ASIA CONSTRUCTION

lighting today

TRADE LINK MEDIA PTE LTD

101 Lorong 23 Geylang #06-04 Prosper House Singapore 388399 Tel: (65) 6842 2580 Fax: (65) 6745 9517
info@tradelinkmedia.com.sg | www.tradelinkmedia.biz

Looking At Cloud Security As A Shared Responsibility

Misconfigured cloud environments are increasingly identified as the source of damaging data breaches and leaks, raising serious questions for enterprises. Where does responsibility for data security in the cloud lie, and how can security professionals best work with their teams and cloud providers to resolve the problem?

By Paddy Francis, CTO for Airbus CyberSecurity

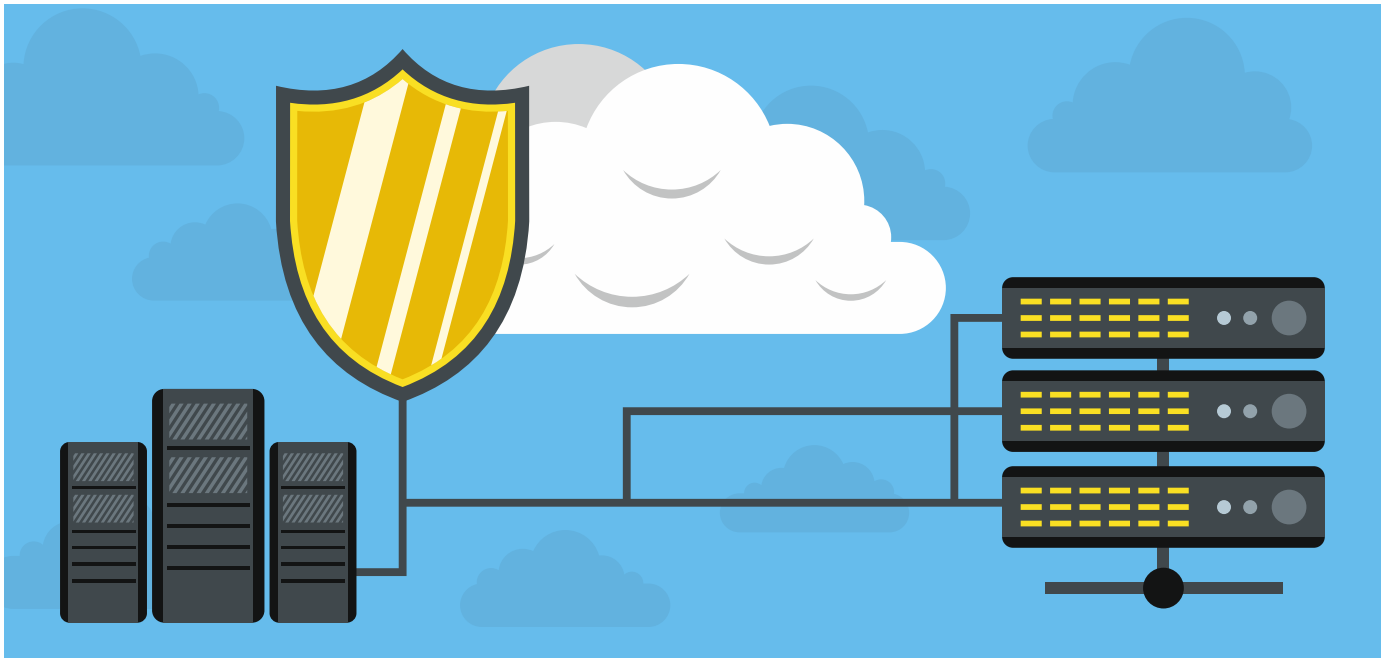
Many organisations, large and small, are moving their data and processing to the cloud to take advantage of the flexibility, efficiency and cost savings it can bring. However, there is sometimes a misconception that the move to cloud also relieves the organisation from responsibility for security. Also, the security management of cloud instances is different from fixed infrastructure and can be complex and unfamiliar. As a result, there have been many examples of security breaches caused by misconfiguration of cloud services, and these are rising year on year.

Responsibility for cloud security varies depending on the type of cloud service, and each provider has a different model. However, at a high level, the following can be applied:

For infrastructure as a service (IaaS), the physical infrastructure, network interfaces, processing and hypervisors are managed by the provider, with the customer being responsible for securing and managing the virtual network, virtual machines, operating systems, middleware, applications, interfaces and data.

For platform as a service (PaaS), the provider takes on more responsibilities, but the customer is still responsible for applications, interfaces and data.

For software as a service (SaaS), the customer's responsibility is reduced to the security of interfaces and data.



In all cases, the customer is responsible for access control, which is where most of the misconfigurations materialise. Also, most enterprises will operate more than one of these models, depending on their business.

Take Care In Choosing A Cloud Provider

There will, of course, remain some on-premise infrastructure that needs to be protected, as well as remote users. Small to medium-sized enterprises (SMEs) will typically allow remote users to connect direct to the cloud so they have virtually no infrastructure of their own. In fact, very small organisations may, in effect, only have remote users, with everybody connecting directly to the cloud via 4G or Wi-Fi.

However, for larger enterprises, particularly those retaining on-site infrastructure, many prefer to have remote users connect back into their home site so that they can be fully authenticated using multifactor authentication before going on to access cloud or other resources using a single sign-on system. The same would apply to any external suppliers, or partners that are allowed access. Here, a cloud access security broker which sits between the cloud service provider and the service consumer can also help extend the controls of the on-premise infrastructure into the cloud.

As the shared security responsibilities will be different for different providers, it is important to identify your security needs before approaching cloud providers so that you can make a proper assessment of what your share of the responsibilities will be for each provider.

Once you have chosen a provider, the key message to get across is that cloud configuration is security critical and must be controlled. At the same time, it is important not to kill the benefits of cloud with overzealous controls. The best approach is to bring together information security, infrastructure management organisations, the security operations team and representatives of any DevOps teams. They can then be briefed, and an agreement can be reached on how the problem will be managed, and identify contributions from each team.

Prepare A Comprehensive Cloud Configuration Plan

Cloud configuration can be complex, so it is essential to prepare a comprehensive plan and ensure that those responsible for configuration are fully trained and that appropriate support is available.

Before going live, the configuration should also be verified to ensure it is in line with the planning and that it is effective and achieving your security aims. This could be done using third-party tools or by external security testers. The latter often add value by finding things that were missed in the original security plan.

Due to the cloud being standardised, there are several third-party tools that will allow monitoring of the configurations constantly. This will help early identification of any misconfigurations. Network traffic monitoring and user behaviour analytics (UBA) can also be used to identify anomalies and misconfigurations, as well as issues that arise due to misconfigurations.

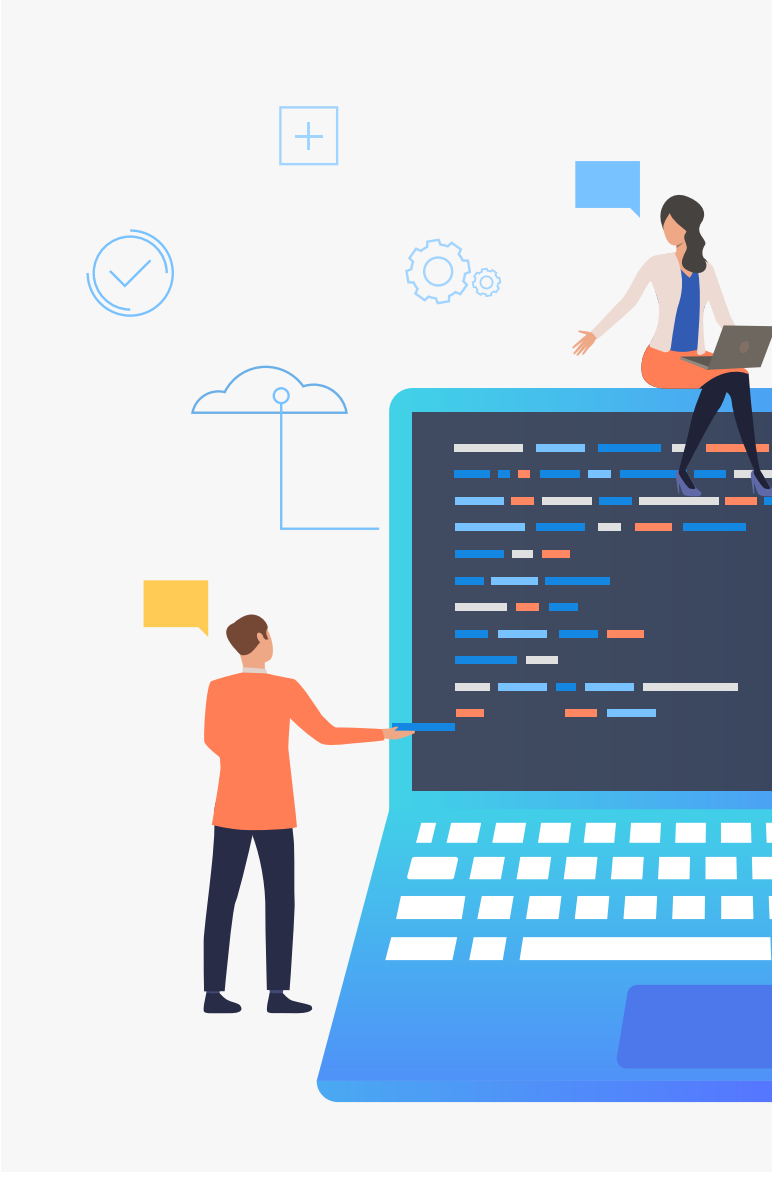
In summary, as with any infrastructure, security must be planned in from the start. This starts before the selection of a provider. You can only secure something you understand, so training and support are essential to enable the system to be configured securely. Finally, verify, test and monitor to ensure the security controls are achieving their objectives.

Security By Design: A Necessity For Cloud

Security by design ensures that IT security is inherent in an organisation's operations and should be adopted when outsourcing services to the cloud.

By Simon Persin, Turnkey Consulting

Cloud environments and the storage of business-critical data within them carry inherent risk. These risks have been exacerbated by the rise of shadow IT, which makes it easy and inexpensive for anyone in the organisation with discretionary spend to purchase cloud-based applications to support their business operations, without necessarily subjecting them to the same level of rigour that is applied before enterprise-level cloud services are selected and implemented.



Defining Data Responsibilities

As with all data security risks, the responsibility lies with the organisation that has collected the data (the data controller in a General Data Protection Regulation [GDPR] world) to ensure it is processed, stored and transmitted securely. Outsourcing IT work and functions does not mean the risk is automatically outsourced.

However, there is some variation on responsibilities, based on the nature of the cloud service provided by a third party. There is little onus on data security for the supplier of cloud-based IT infrastructure (IaaS), for example, because it offers only the basic system structure on which the customer builds its own IT environment. While the provider might be responsible for general maintenance and the overall security of the IT system, it is not in charge of the data itself. The story is similar for cloud platforms (PaaS), which supply tools to further facilitate the customer's needs.

Where the situation becomes more fluid is at the application level, as the cloud provider has a more active role in the operation of the service and may therefore have access to the data contained within it.

And while many of the cloud provisioning services take great pains to secure the information they are processing,

storing and transmitting, an organisation cannot be complacent when it comes to protecting the data it has in the cloud.

Doing The Groundwork

The first step is to undertake the appropriate level of due diligence on the cloud service supplier to ensure that data will be managed securely so that the interests of both the customer and its clients will be protected. Front of mind from the outset should also be having the right controls—both process and technical—in place to manage any risks that do exist, particularly where data held may be of a sensitive nature, such as personal information.

Privacy regulations must also be taken into account. For example, the personal data of EU citizens comes under the jurisdiction of the GDPR (currently the most prevalent legislation). Responsibility for this personal information is placed on the data controller (the customer) to ensure that processing of data is compliant, while the data processor (the cloud provider) must take accountability for some of the information being handled—because data stored in the cloud is shared more widely than that in traditional on-premise environments—and the ultimate liability remains with the controller.

The focus should be on appropriate data classification up front, defining the correct level of responsibility and ensuring that those requirements are communicated clearly as contractual responsibilities. Once everyone is aware of the need to protect the information, appropriate measures to do so can be identified, documented and tested to protect the information stored. This includes processes for notification in cases of breaches and response plans in case the worst case happens.

Public Cloud And Shared Responsibility

Many organisations opt to use a public cloud provider, rather than a private one, for some or all of their requirements, and this can change the responsibility dynamic. Amazon Web Services (AWS), for example, is transparent that responsibility for data security and compliance is shared between it and the customer. AWS operates, manages and controls the components from the host operating system, while the customer assumes responsibility and management of the guest operating system (including updates and security patches), other associated application software, and the configuration of the AWS-provided security group firewall. Further responsibility divides are determined by the services used.

AWS also provides a number of in-built tools that the customer can use to remediate and mitigate any potential risks. There is also a level of support provided, which can remediate most security risks and provide feedback as to how the customer can improve their security and compliance, if required.

Building Security By Design Into The Supplier Lifecycle
Security by design ensures that IT security is inherent in an organisation's operations and is an approach that can be adopted when outsourcing services to the cloud. The following checklist covers the key points to address:

- **Internal understanding:** The customer needs to be aware of the types of information it is storing in the cloud environment and its sensitivity.
- **Pre-contract checks:** Confirmation that the cloud provider has the basic security elements in place that enable it to meet required standards, such as handling the data being stored/processed/transmitted, and so on, in a way that is appropriate to its sensitivity.
- **Contractual clauses:** Predefined clauses covering issues such as breach notification, breach of contract in the event of incidents, metrics that the cloud provider must report, and possibly right to audit, can be inserted.
- **Ongoing contract:** Key performance indicators (KPIs) on which the cloud provider needs to report (number of people/locations with access, risks the third party manages behalf of the customer, confirmation of vulnerability scans/patches, for example) and that the actions (especially closing leavers accounts) are performed quickly.
- **Business dialogue:** Internal customer discussions to understand whether business users have adopted applications or services outside IT's remit (shadow IT) that require additional steps to be taken to secure organisational data.
- **Audit reports:** SoC 2 audit reports should be received and reviewed where relevant.
- **Contract changes:** Controls and the contract need to change as the cloud provider adapts the service over time to meet the customer's needs.
- **Offboarding contract:** Confirmation of data disposal and the return of intellectual property (IP) to the customer.

Everyone Is Responsible For Data Security

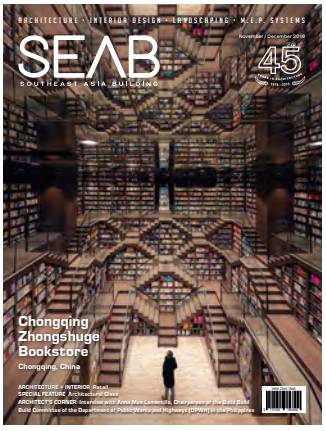
IT security professionals have a significant role to play in ensuring that the right standards are met in all aspects of cloud service provision so that it benefits the organisation without introducing risk that is, at best, unnecessary and, at worst, counterproductive.

From a technical perspective, this includes undertaking thorough testing of cloud services and putting the right controls in place to mitigate the risks that do exist. But it is also about fostering understanding throughout the business so that people see how their individual actions, such as using unauthorised applications, can have a direct impact on the overall enterprise.

SUBSCRIPTION FORM

Fax your order to **+65 6842 2581** or email us at **info@tradelinkmedia.com.sg**

Please (√) tick in the boxes.



☐ **Southeast Asia Building**
Since 1974

☐ **Southeast Asia Construction**
Since 1994

☐ **Security Solutions Today**
Since 1992

***1 year** (6 issues) per magazine*

Singapore	SGD$60.00
Malaysia / Brunei	SGD$105.00
Asia	SGD$155.00
America, Europe	SGD$185.00
Japan, Australia, New Zealand	SGD$185.00
Middle East	SGD$185.00

☐ **Bathroom + Kitchen Today**
Since 2001

***1 year** (4 issues)*

Singapore	SGD$32.00
Malaysia / Brunei	SGD$70.00
Asia	SGD$85.00
America, Europe	SGD$135.00
Japan, Australia, New Zealand	SGD$135.00
Middle East	SGD$135.00

Lighting Today
Since 2002

Lighting Today is available on digital platform.To download free PDF copy please visit:

http://lt.tradelinkmedia.biz

Personal Particulars

Name: _____

Position: _____

Company: _____

Address: _____

_____

Tel: _____ Fax: _____

E-Mail: _____

IMPORTANT

Please commence my subscription in

_____(month/year)

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
Co. Reg. 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: _____

PLATINUM PARTNER

Dahua Technology | Singapore | +65 6538 0952 | sales.sg@dahuatech.com | www.dahuasecurity.com | IFC, 1

GOLD PARTNERS

Microengine Technology | Malaysia | +603 7957 2008 | enquiry@microengine.net | www.microengine.net | 5

SILVER PARTNER

Johnson Controls | Singapore | +65 6319 9820 | bts-apac-detection-products@jci.com | www.zettlerfire.com | 3

See us at these upcoming events!

Event	Date	City	Country	Website	Page
ISC West 2020	18 - 20 Mar 2020	Las Vegas	U.S.A.	www.iscwest.com	13
Megabuild 2020	19 - 22 Mar 2020	Jakarta	Indonesia	www.megabuild.co.id	15
Secutech India 2020	7 - 9 May 2020	Mumbai	India	www.secutechexpo.com	7
IFSEC International 2020	19 - 21 May 2020	London	United Kingdom	www.ifsec.events/international/	IBC
IFSEC SEA 2020	23 - 25 Jun 2020	Kuala Lumpur	Malaysia	www.ifsec.events/kl/	9
IFSEC Philippines 2020	22 - 24 July 2020	Manila	Philippines	www.ifsec.events/philippines/	11
GSX 2020	21 - 23 Sep 2020	Atlanta	U.S.A.	www.gsx.org	OBC

IFSEC INTERNATIONAL

informa markets

SAVE THE DATE

IFSEC International returns

19-21 May 2020, ExCeL London

Co-located with:

FIREX INTERNATIONAL

SAFETY & HEALTH EXPO

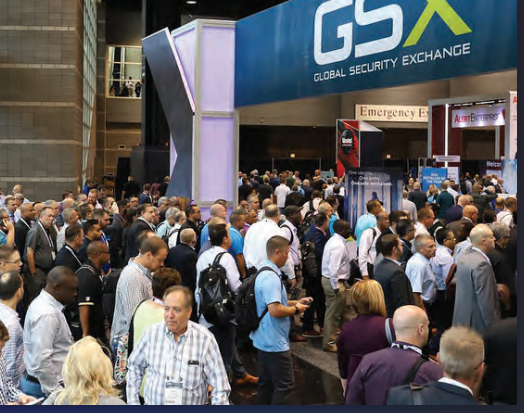
FACILITIES SHOW

Plus:

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

FORENSICS EUROPE EXPO 19-21 May 2020 ExCeL, London

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



GSX

GLOBAL SECURITY EXCHANGE

FORMERLY ASIS ANNUAL SEMINAR & EXHIBITS

21–23 SEPTEMBER 2020

GEORGIA WORLD CONGRESS CENTER
ATLANTA, GA

GSX.ORG | #GSX20

At GSX2020, thousands of executives and decision makers will be actively assessing the latest security technologies and solutions.

And...

MORE THAN 40%

of them don't attend other events.*

Let's discuss how we can support your business development goals.

SECURE YOUR BOOTH SPACE TODAY »
GSX.org/exhibit