MAR / APR 2020

# SECURITY SOLUTIONS TODAY


## SAFE CITIES, THE SMART WAY

**In Focus**
How To Navigate A Ransomware Recovery Process

**In Focus**
Tips For Ransomware Protection On Windows Systems

**Security Feature**
Small Business Cybersecurity Threats And How To Fix the Fox

**Security Feature**
Intrusion And Access Control: The Perfect Pair For Facility Security



# 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**

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

# IN THIS ISSUE





# 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

# CONTACT

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

**ASSOCIATE PUBLISHER**
Eric Ooi
(eric.ooi@tradelinkmedia.com.sg)

**EDITOR**
CJ Chia
(sst@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)


Photo by JC Gellidon on Unsplash
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)

**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



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

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

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

# 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

# COMING SOON

**MAR 18 – 20 2020**

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

**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 02– 05 2020**

**AusCERT Cyber Security Conference**
Gold Coast, Australia
- https://conference.auscert.org.au/
conference@auscert.org.au

**JUN 23 – 25 2020**

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

**JUL 06 – 07 2020**

**Cyber Security Asia Malaysia**
Kuala Lumpur, Malaysia
+603 22606500 https://cybersecurityasia.tech/
admin@thomvell.com, karen@thomvell.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 01 – 06 2020**

**Black Hat USA**
Las Vegas, USA
+1 866 203 8081 https://www.blackhat.com/us-20/
blackhatregistration@ubm.com

**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

# SAFETY & SECURITY ASIA 2020

The 19TH International Safety & Security Technology & Equipment Exhibition

## 6 - 8 October 2020

Halls D, E & F, Sands Expo & Convention Centre
Marina Bay Sands, Singapore

Be a part of Safety & Security Asia 2020 - the quality sourcing platform for excellent commercial security solutions. Showcase your latest technologies, innovations and safety and security services in the most established and longest-running commercial security trade show in ASEAN!

### JOIN SSA 2020 TODAY TO

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

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

A Part Of

Architecture & Building Services 2020
Design Solutions for the Built Environment

Organised By

CEMS
Conference & Exhibition Management Services Pte. Ltd.

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

# Dear readers,

Cities around the world house more than half of our entire population, and as we see increased urbanisation, this is a number that will continue to grow. With the population density in city areas being much higher than that of rural areas, keeping every inch of the city safe is a massive undertaking, but it is one that cannot be avoided.

But what does it mean to be a Safe City? There are multiple considerations that must be met to maintain a safe and secure urban space. Something as simple as someone feeling safe enough to walk alone at night needs many facets of security to come together; the path needs to be well-lit so as to reduce the likelihood of the person tripping; proper footpaths must be in place so that a person has less risk of being hit by vehicles. The environment in a city must be safe for people to live, work, and play in, and the population must have access to healthcare to keep them healthy.

The development of new technology has evolved the ways through which cities might be kept safe, but technology has also created new risks for the safety of those living within cities. In this issue, we look at the different pillars of safety in cities, how technology has changed the face of a safe city, as well as the security concerns that result.

This issue, we'll also delve into how smart solutions affect businesses through the creation of more seamless workplaces; the security challenges that result from the implementation of digital innovations.

We check out some perimeter security and intrusion detection solutions that are available on the market and some of the useful applications for these solutions. And finally, we dig deeper into how to navigate the threats presented by ransomware in the digital age. Happy reading!

CJ Chia

Editor

*Designed by pikisuperstar / Freepik*

# OUR WEBSITE HAS A FRESH NEW LOOK.

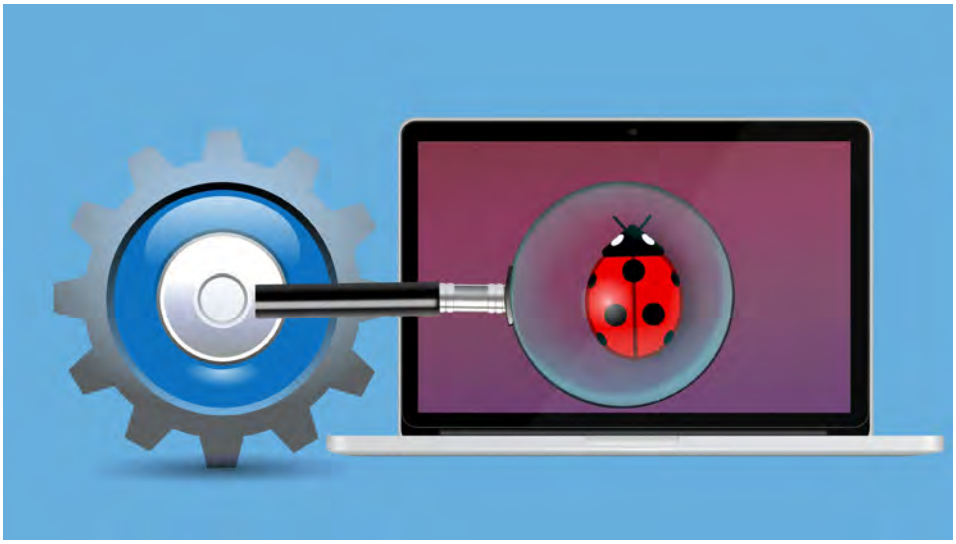




sst.tradelinkmedia.biz

# KUBERNETES SECURITY GETS AN ASSIST WITH BUG BOUNTY PROGRAM

The Cloud Native Computing Foundation wants to entice a broader community of independent researchers to work on Kubernetes security with a bug bounty program launched this week.



The program, which will see bug bounty vendor HackerOne take over Kubernetes security bug triage and verification from the Kubernetes Security Product Group, will offer rewards for independent security researchers of between $100 and $10,000.

The idea of a bug bounty program to boost Kubernetes security has been in discussions within the open source community since 2018, and last year a community RFP process selected HackerOne over Bugcrowd to administer the program. The Cloud Native Computing Foundation (CNCF) also conducted a public Kubernetes security audit last year.

Bug bounty programs, while widely used, vary in effectiveness, but IT pros that work with Kubernetes approved of the program rollout this week.

"Incentivising the crowd to help identify and provide reproducible issues has benefits for any open source software project," said Chris Riley, DevOps delivery director at Cprime Inc., an Agile software development consulting firm in San Mateo, Calif. "The Kubernetes Security Product Group then has a pipeline of reported issues that are ready to reproduce, and they can focus on the resolution."

That was the major impetus for the decision to enlist HackerOne and launch the bug bounty program, according to Kubernetes Security Product Group members. The program is open to Kubernetes developers, but as Kubernetes matures and is more widely used, the community must expand beyond its core developer base to find security issues.

"The hope is that the bug bounty program will help us attract more of the security-focused research community, and help us draw attention to parts of the product that don't get as much attention from regular developers," said Tim Allclair, staff software engineer at Google and chair of the SIG-Auth group that oversees Kubernetes security.

For example, the open source supply chain for Kubernetes could use further security evaluation, Allclair said.

"We want to make sure that all code that's contributed is properly vetted," he said. The response to the bug bounty program, and any Kubernetes security issues it brings to light, will steer the activities of the Kubernetes Security Product Group in 2020.

CNCF declined to comment on the size of overall funding for the Kubernetes bug bounty program. Rewards of up to $10,000 are in line with other open source bug bounty programs, such as the Internet Bug Bounty.

The CNCF chose HackerOne over BugCrowd in January 2019, according to community documents, because of tight integration with GitHub and simple vulnerability report disclosure and automated response workflows. The RFP process and establishment of the bug bounty program came in the wake of a critical vulnerability in the container orchestration software disclosed in December 2018.

While the bug bounty program won't hurt, IT security analysts say it might not have a huge effect on Kubernetes security in general.

"Bug bounty programs don't replace things like the public security audit for Kubernetes and getting paid isn't a primary motivator for a lot of security researchers," said Daniel Kennedy, analyst at 451 Research.

Instead, security researchers are attracted to bug bounties because they offer a systematic process to report bugs and receive fixes in a specific timeframe – something the Kubernetes Security Product Group already did. "It's noteworthy, and seems to have been applied properly, but I don't know that they'll get a huge pop out of it," Kennedy added.

# GEOTAB ANNOUNCES LAUNCH OF INTEGRATED GENERAL MOTORS TELEMATICS SOLUTION

Geotab, a global leader in IoT and connected transportation, announced the availability of the Geotab Integrated Solution for General Motors (GM).

The solution, which launched at Geotab's largest Connect conference to date, allows fleet managers to access their compatible Chevrolet, Buick GMC, and Cadillac vehicle data within the MyGeotab platform via a factory-fit, GM-engineered embedded OnStar module, providing fleet managers with access to one dedicated portal of powerful tools to meet all connectivity needs for today's fleets.

With no installation or additional hardware required, the latest solution from Geotab and GM simplifies the task of mixed-fleet management by providing businesses with the ability to oversee their entire fleet from within one platform. With this solution, fleet managers will gain access to rich, proprietary GM-specific data for connected Chevrolet, Buick, GMC and Cadillac models 2015 or newer, equipped with the compatible OnStar module in the United States to help optimise fleet productivity, compliance, and safety.

"GM Fleet and Geotab have many of the same customers and we want to provide them with the tools they need to run their business effectively and efficiently," said Ed Peper, U.S. vice president of GM Fleet.

"The Geotab Integrated Solution for GM will enable fleet managers to have increased visibility into vehicle productivity, location data and more."

Vehicles able to access the Geotab Integrated Solution for GM will have the added benefit of access to the Geotab Marketplace—an exclusive online portfolio of mobile apps, hardware add-ons and software add-ins that enable Geotab customers to further customise their fleet management solution. The solution is currently only available in the U.S. with plans to expand to include vehicles in Canada in the coming months.

"GM is committed to leading the transformation of the automotive industry, and we're proud to partner with them," said Geotab Vice President of Strategic Partners Sherry Calkins.

# IBM EXPANDS PATENT TROLL FIGHT WITH ITS MASSIVE IP PORTFOLIO

After claiming more than a quarter century of patent leadership, IBM has expanded its fight against patent assertion entities, also known as patent trolls, by joining the LOT Network. As a founding member of the Open Invention Network in 2005, IBM has been in the patent troll fight for nearly 15 years.

The LOT Network (short for License on Transfer) is a non-profit community of more than 600 companies that have banded together to protect themselves against patent trolls and their lawsuits. The group says companies lose up to $80 billion per year on patent troll litigation. Patent trolls are organisations that hoard patents and bring lawsuits against companies they accuse of infringing on those patents.

IBM joins the LOT Network after its $34 billion acquisition of Red Hat, which was a founding member of the organisation.

"It made sense to align IBM's and Red Hat's view on how to manage our patent portfolio," said Jason McGee, vice president and CTO of IBM Cloud Platform. "We want to make sure that patents are used for their traditional purposes, and that innovation proceeds and open source developers can work without the threat of a patent litigation."

To that end, IBM contributed more than 80,000 patents and patent applications to the LOT Network to shield those patents from patent assertion entities, or PAEs.

IBM joining the LOT Network is significant for a couple of reasons, said Charles King, principal analyst at Pund-IT in Hayward, California. First and foremost, with 27 years of patent leadership, IBM brings a load of patent experience and a sizable portfolio of intellectual property (IP) to the LOT Network, he said.


"IBM's decision to join should also silence critics who decried how the company's acquisition of Red Hat would erode and eventually end Red Hat's long-standing leadership in open source and shared IP," King said. "Instead, the opposite appears to have occurred, with IBM taking heed of its new business unit's dedication to open innovation and patent stewardship."

The LOT Network operates as a subscription service that charges members for the IP protection they provide. LOT's subscription rates are based on company revenue. Membership is free for companies making less than $25 million annually. Companies with annual revenues between $25 million and $50 million pay $5,000 annually to LOT. Companies with revenues between $50 million and $100 million pay $10,000 annually to LOT. Companies with revenues between $100 million and $1 billion pay $15,000. And LOT caps its annual subscription rates at $20,000 for companies with revenues greater than $1 billion.

Meanwhile, the Open Invention Network (OIN) has three levels of participation: members, associate members, and licensees. Participation in OIN is free, the organisation said.

"One of the most powerful characteristics of the OIN community and its cross-license agreement is that the board members sign the exact same licensing agreement as the other 3,100 business participants," said Keith Bergelt, CEO of OIN. "The cross license is royalty-free, meaning it costs nothing to join the OIN community. All an organisation or business must agree to do is promise not to sue other community participants based on the Linux System Definition."

IFI Claims Patent Services confirms that 2019 marked the 27th consecutive year in which IBM has been the leader in the patent industry, earning 9,262 U.S. patents last year. The patents reach across key technology areas such as AI, blockchain, cloud computing, quantum computing, and security, McGee said.

IBM achieved more than 1,800 AI patents, including a patent for a method for teaching AI systems how to understand implications behind certain text or phrases of speech by analysing other related content. IBM also gained patents for improving the security of blockchain networks.

In addition, IBM inventors were awarded more than 2,500 patents in cloud technology and grew the number of patents the company has in the nascent quantum computing field. "We're talking about new patent issues each year, not the size of our patent portfolio, because we're focused on innovation," McGee said. "There are lots of ways to gain and use patents, we got the most for 27 years and I think that's a reflection of real innovation that's happening."

Since 1920, IBM has received more than 140,000 U.S. patents, he noted. In 2019, more than 8,500 IBM inventors, spanning 45 different U.S. states and 54 countries contributed to the patents awarded to IBM, McGee added.

In other patent-related news, Apple and Microsoft this week joined 35 companies who petitioned the European Union to strengthen its policy on patent trolls. The coalition of companies sent a letter to EU Commissioner for technology and industrial policy Thierry Breton seeking to make it harder for patent trolls to function in the EU.

# CLEARVIEW HACK FUELS DEBATE OVER FACIAL RECOGNITION

Clearview holds in excess of three billion photos of people in its database. It has scraped these images from the public internet (including social media) without ever seeking explicit permission from any of the people pictured. Its modus operandi is to sell access to this database to law enforcement agencies, with the goal of making it easier for police to identify suspects using its machine learning and artificial intelligence (AI) algorithms to compare photos.
It claims: "Clearview's technology has helped law enforcement track down hundreds of at-large criminals, including paedophiles, terrorists and sex traffickers. It is also used to help exonerate the innocent and identify the victims of crimes including child sex abuse and financial fraud."
However well-intentioned, its behaviour has already prompted outrage. In January, The New York Times published an in-depth exposé of Clearview – which was founded by Hoan Ton-That, a Vietnamese-Australian college drop-out and former fashion model, and backed by, among others, Peter Thiel of Palantir.


Besides the scraping of photos without consent, the newspaper uncovered a worrying culture at Clearview. Among other things, The New York Times alleged that Ton-That had created fake identities to throw its reporter off the scent, and encouraged police officers to intimidate and harass them. He also sought funding from white supremacist businessman and failed US politician Paul Nehlen.
As a result of the negative publicity it has attracted, Clearview is already attracting lawsuits over its collection and storage of biometric identifiers without consent, and digital platforms including Google and Twitter have ordered it to cease and desist its activities.

According to the Daily Beast, which was one of the first news outlets to report on the hack after receiving leaked communications informing customers of the breach, an intruder gained unauthorised access to Clearview data, including its customer list, the number of user accounts they had set up, and the number of searches they had run through its systems.

Clearview claimed there was no breach of its servers or compromise of its systems or network, and that the vulnerability has since been fixed.

In a statement sent to the news outlet, company attorney Tor Ekeland said: "Security is Clearview's top priority. Unfortunately, data breaches are part of life in the 21st century. Our servers were never accessed. We patched the flaw and continue to work to strengthen our security."
Tim Mackey, principal security strategist in the cyber security research centre (CyRC) at Synopsys, said that in general there were two types of attacks – opportunistic and targeted – and it was clear which type the Clearview hack was.

"With the type of data and client base that Clearview AI possesses, criminal organisations will view compromise of Clearview AI's systems as a priority. While their attorney rightly states that data breaches are a fact of life in modern society, the nature of Clearview AI's business makes this type of attack particularly problematic," said Mackey.

"Facial recognition systems have evolved to the point where they can rapidly identify an individual, but combining facial recognition data with data from other sources like social media enables a face to be placed in a context which, in turn, can enable detailed user profiling – all without explicit consent from the person whose face is being tracked," he added. "There are obvious benefits for law enforcement seeking to identify missing persons to use such technologies for good, but with the good comes the bad."

Forrester senior analyst Kjell Carlsson said there was a high likelihood that whoever was behind the hack would leak the client list, likely seeking to feed the public backlash against Clearview.

"It will likely bring the public awareness, and mistrust, of facial recognition to a new level. We can expect many knee-jerk reactions that try to bar law enforcement from using facial recognition. Much of this legislation will prove ineffective because it is unable to distinguish new facial recognition technologies from the earlier solutions that police have been using for decades, but it will be a deterrent for local governments to investigate and invest in these solutions," he said.

Carlsson said it was unlikely that the incident would lead to a slowdown in the use of facial recognition and related technologies. He said the technology was too useful and convenient to deter widespread adoption, citing more mundane uses such as replacing swipe cards to enter office buildings, or even paying for things, which is becoming popular in China. "If there is one thing that Facebook has shown it is that customers are extremely willing to forgo privacy for convenience," he said.

# FOUR-FIFTHS OF SIM-SWAP FRAUD ATTEMPTS SUCCESSFUL

A study by Princeton University has revealed that the authentication procedures used by five leading US pre-paid carriers when a customer attempted to change their SIM card used insecure authentication challenges that could be easily subverted by attackers.

The study, an empirical study of wireless carrier authentication for SIM swaps, by Kevin Lee, Ben Kaiser, Jonathan Mayer and Arvind Narayanan, set out from the baseline that the procedures in question were an important line of defence against attackers. These attackers seek to hijack victims' phone numbers by posing as the victim and calling the carrier to request that service be transferred to a SIM card the attacker possesses.

The team noted that SIM-swap attacks allow attackers to intercept calls and messages, impersonate victims, and perform denial-of-service (DoS) attacks, and added that they have been widely used to hack into social media accounts, steal cryptocurrencies, and break into bank accounts.

Warnings have existed since 2016 distinguishing SMS-based authentication from other out-of-band authentication methods due to heightened security risks, including SIM change.

Princeton examined the types of authentication mechanisms in place for such requests at five US pre-paid carriers – AT&T, T-Mobile, Tracfone, US Mobile, and Verizon Wireless – by signing up for 50 prepaid accounts, 10 with each carrier, and subsequently calling in to request a SIM swap on each account.

The methodology used to quantify the downstream effects of the vulnerabilities saw the research team reverse-engineer the authentication policies of more than 140 websites that offer phone-based authentication.

The team rated the level of vulnerability of users of each website to a SIM-swap attack. It found 17 websites on which user accounts can be compromised based on a SIM swap alone, such as without a password compromise.

The key finding from the research was that all five carriers used insecure authentication challenges that could easily be subverted by attackers. Princeton also found that in general, callers only needed to successfully respond to one challenge to authenticate, even if they had failed numerous prior challenges.

In each carrier, procedures were generally consistent, although on nine occasions across two carriers, customer service representatives (CSRs) either did not authenticate the caller or leaked account information prior to authentication.

The research also discovered that attackers generally only needed to target the most vulnerable authentication challenges because the rest could be bypassed.

In an evaluation of post-paid accounts at three carriers, the researchers said that they may have found some evidence that some carriers have implemented stronger authentication for post-paid accounts than for pre-paid accounts.

In July 2019, Princeton provided an initial notification of the findings to the carriers it studied and to the US trade association representing the wireless communications industry, the CTIA. In January 2020, T-Mobile informed Princeton that after reviewing its research, it has discontinued the use of call logs for customer authentication.

In a call to action following the research, Princeton advised carriers to discontinue the methods of customer authentication they were using and implement more secure practices.

In addition to calling on carriers to provide optional heightened security for customers, the team implored them to restrict customer support representative access to information before customers authenticated.

The researchers also recommended that websites employ threat modelling to identify vulnerabilities and implement at least one secure multi-factor authentication option.

Analysing the data, Aseem Sadana, group chief operating officer (COO )at cloud communications software and solutions provider IMImobile, observed that SIM-swap fraud was a big concern for the industry, and that the study from Princeton University highlighted that there was still a lot of work to be done.

"Despite advances in technology, SIM-swap fraud continues to be difficult to detect and prevent, as fraudsters are adapting their techniques," he said. "As such, mobile operators and banks need to work together to ensure their processes for detecting fraudulent activity are constantly evolving.

"When it comes to customer data, such as SIM card information, device type and location, mobile operators and banks must be able to run checks in real-time, but at the moment many fraud prevention systems are still reliant on historical data.

"If they work with customer engagement specialists, both parties can put better practices and technologies in place to combat SIM-swap fraud, enabling them to identify risk before customers lose money," he added.

# RING ANNOUNCES NEW SECURITY, PRIVACY SAFEGUARDS FOR CUSTOMERS

Following several well-publicised hacking incidents and outcry from privacy advocates about its app sharing user information with third parties, video doorbell maker Ring last week announced that it will offer additional account security for all of its customers.

Ring, which is owned by tech and retail giant Amazon, said that while two-factor authentication was already an option provided to all customers, it is now making a second layer of verification mandatory for all users when logging into their accounts.

Now every time a user logs into their account, they will receive a one-time, six-digit code to verify the attempt. In addition, Ring announced that it would be "temporarily pausing" the use of most third-party analytics services in the Ring app and website while they work to provide customers with more abilities to opt out in its Control Centre. The company also said that customers can now opt of sharing their information with third-party service providers for the purpose of receiving personalised ads.

"Your account safety and security is our priority. We will stay vigilant and continue to give you more transparency and control over your devices and personal information, and help keep your home and Ring account secure and protected," Ring President Leila Rouhi said in the statement announcing the new safeguards.

Though it acknowledged the moves as a "good step forward," the Electronic Frontier Foundation (EFF), one of the civil liberties groups that has levied privacy criticisms against Ring in the past, said there are still a number of reforms the company should undertake if they want to address the "fundamental problems" the group says their technology poses.


Designed by pikisuperstar / Freepik

Among the moves the EFF said the company should make include ending its rapid expansion of law enforcement partnerships across the country; implement measures that require warrants to be issued to device owners for law enforcement to gain access to footage; put limits in place for sharing of video between law enforcement agencies; adjusting default settings to turn off automatic audio recording when the camera is motion activated; and, not integrate facial recognition software into its cameras under any circumstances.

"Ring is creating an environment where every time a person walks down a public street, their movements are being recorded, stored, and made accessible to a whole host of individuals, law enforcement agencies, and Amazon. Ring's technical reforms will better guard the security of customers, but do little to address the bigger threats to privacy that Ring poses," the EFF wrote in a statement.

The announcement by Ring also comes as an increasing number of consumers are clamouring for increased cybersecurity protections from their home security providers.

According to a recent survey conducted by ADT of more than 1,200 U.S. consumers, 92% of respondents said that smart home security companies need to take measures to protect consumers' personal data and information. Among the top cyber concerns reported by survey respondents were hacking (75%), followed by government spying on in-home smart cameras (53%) and smart speakers (52%).

The survey also uncovered that when it comes to how personal information is shared, consumers tend to be more concerned about how governments (89%) and companies (93%) share their personal information than they are about how they share their own personal information on social media (86%). Additionally, despite acknowledging the importance of privacy protocols, most consumers do not use privacy measures available to them; in fact, fewer than 40% of survey respondents reported having any data privacy measures in place at all.

## ZERO-DAY IE BUG IS BEING EXPLOITED IN THE WILD

Both Microsoft and the US government are warning computer users of a critical remote code execution (RCE) vulnerability in Internet Explorer, which is currently being exploited in the wild. The zero-day bug, CVE-2020-0674, exists in the way the scripting engine handles objects in memory in IE, according to a Microsoft advisory updated over the weekend.

Attackers could send phishing emails to victims, tricking them into visiting a specially crafted website designed to exploit the flaw through IE, Redmond claimed.

"The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user," it continued.

"If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights."

The vulnerability affects IE versions 9, 10 and 11 running on all Windows desktop and server versions, including the no-longer supported Windows 7 and Server 2008.

Despite admitting that the flaw is being exploited in "limited targeted attacks," Microsoft has yet to release an emergency patch. Instead, it detailed a set of temporary mitigations which revolve around restricting access to the JavaScript component JScript.dll.

Carl Wearn, head of e-crime at Mimecast, advised organisations to enforce the use of alternative browsers until the issue is fixed.

"In addition to the threat from this zero-day vulnerability, I would also be wary of using IE at present due to the current resurgence in the use of exploit kits specifically designed to exploit IE vulnerabilities," he added.

"Ransomware threat actors in particular are currently utilising exploit kits such as Fallout and Spelevo. While posing no threat to other browsers these exploit kits will likely compromise any Windows machine utilising Internet Explorer if it visits a compromised website."

IE versions still have a combined global market share of over 5%, according to the latest figures from December 2019.

## OVER 2,000 WORDPRESS SITES HIT BY MALICIOUS REDIRECTS

Thousands of WordPress sites have been infected with malicious JavaScript in an attempt to promote scam websites, according to Sucuri.

The number of infections spiked last week, with hackers exploiting vulnerabilities in various plugins, including Simple Fields and the CP Contact Form with PayPal, the security vendor explained in a blog post.

After exploitation, the hackers are able to inject JavaScript which begins a series of redirects to a fraudulent "survey-for-gifts" website, where users are tricked into handing over personal info and unwittingly installing malware.

Among the domains registered as part of the campaign are gotosecond2[.]com, adsformarket[.]com, admarketlocation[.]com and admarketresearch[.]xyz.

"Unfortunately for website owners, this malicious JavaScript payload is capable of making further modifications to existing WordPress theme files via the /wp-admin/theme-editor.php file. This allows them to inject additional malware, such as a PHP backdoors and hacktools, to other theme files so they can continue to maintain unauthorised access to the infected website," Sucuri explained.

"We encourage website owners to disable the modification of primary folders block hackers from inserting malicious files or includes as part of WordPress security hardening and security best practices."

The attackers have also been observed abusing/wp-admin/ features to create fake plugin directories that contain more malware, for example by uploading zip compressed files using the /wp-admin/includes/plugin-install.php file to upload and unzip a compressed fake plugin into /wp-content/plugins/.

The two most common fake plugin directories spotted by Sucuri are /wp-content/plugins/supersociall/supersociall.php and /wp-content/plugins/blockspluginn/blockspluginn.php.

The firm has seen over 2,000 infected sites thus far compromised in this campaign.

WordPress is by far the biggest culprit when it comes to hacked website platforms. It accounted for 90% of compromised websites spotted by Sucuri in 2018, up from 83% in 2018. There was a big drop to Magento (4.6%) and Joomla (4.3%) in second and third.

# SKYLO EMERGES FROM STEALTH WITH WORLD'S MOST AFFORDABLE SATELLITE NETWORK FOR IoT DATA


Skylo, maker of the world's most affordable and ubiquitous network that connects any machine or sensor, announced that the company has emerged from Stealth with $116 million in total funding. The company previously raised $13 million in a Series A round that was co-led by DCM and Innovation Endeavors, and joined by Moore Strategic Ventures. The new Series B round raised $103 million, led by SoftBank Group and joined by all existing investors.

Skylo will bring instant, affordable and ubiquitous Internet of Things connectivity to millions of machines, sensors and devices, even in the most remote geographies. It is the world's first company to leverage the cellular Narrowband Internet of Things (NB-IoT) protocol via satellite, making it possible to instantly connect billions of sensors on objects and machines in remote areas. Skylo's new satellite connectivity leverages existing geostationary satellites to bring reliable connectivity without the need to add new infrastructure in space. Skylo has successfully built and proven its end-to-end technology and completed successful commercial field trials with major enterprise and government customers. The company's customers already include enterprise and government entities in a range of industries including automotive, railways, agriculture and maritime.

Skylo costs 95% less than existing satellite solutions, with connectivity starting at just $1 per user and hardware that costs less than $100. Skylo is the world's most affordable satellite technology and will enable operations for remote businesses, increase safety, drive economic development and job creation, and help with disaster preparedness and response.

"Skylo envisions a world where connectivity for machines, sensors and devices is as ubiquitous as the sky," said Skylo co-founder and CEO Parthsarathi "Parth" Trivedi. "This low-cost, global fabric of connectivity for machine data will be transformative for entire industries."

The use cases for Skylo are diverse and transformational for industry and government customers:

**Mobilising data for shipping and logistics**

- Telemetry sensors are increasingly being built into and retrofitted onto trucks and railway cars, but the connectivity needed to make the data actionable has been missing. By equipping them with Skylo's geographically ubiquitous connectivity, customers have a way to access real-time delivery updates, ensure the integrity of temperature-sensitive deliveries (like pharmaceuticals or food), monitor maintenance schedules, certify safety compliance, and more.

**Improving agriculture crop health and productivity**

- Skylo allows farmers to optimise operations by sending and receiving real-time data about growing conditions such as air temperature, moisture level or soil pH. The data can inform watering schedules, fertiliser needs, and growth cycles, resulting in lower energy costs, less water usage, and healthier crops. Skylo also supports emerging business models for equipment sharing, enabling "tractor sharing," for instance. In this case, farmers and equipment owners can connect to and share heavy-duty machinery, which enables hundreds of millions of farmers to increase their productivity because of affordable access to farming equipment.

**Digitising the fisheries industry**

- Globally, there are 4.6 million fishing vessels1 that can now be connected for the first time over Skylo. Skylo's Hub connects to existing Android devices over Bluetooth or Wi-Fi, allowing fishermen to access life-saving two-way SOS communications, connect with their fleet operator, and access markets to transact their catch while still at sea.

**Connectivity for modern passenger transportation systems**

- Railway systems, long-distance buses, and other vehicles can use Skylo to transmit vehicle health data required for on-time performance and operational efficiency. Skylo can enable the delivery of preventative maintenance alerts and even saves lives by triggering alerts in the case of an abnormal track vibration, sudden braking or acceleration or sharp turns.

Skylo's end-to-end solution encompasses the Skylo Hub, the Skylo Network, the Skylo Data Platform and Skylo API. Mass manufacturing of the Skylo Hub is underway and the Skylo Network is already live with early customers.

Skylo will scale customer implementations first in India and other emerging markets, where it has already started implementing the technology in a range of industries. Skylo's service will be commercially available later this summer and the company is in commercial trials with users in the U.S. and other world regions for subsequent launches and market expansion.

## TELEFÓNICA CERTIFIES QUECTEL'S NB-IOT MODULE WITH SUBSCRIPTION SWAP CAPABILITIES

Quectel Wireless Solutions, a leading global supplier of Internet of Things (IoT) modules, has been collaborating with Telefónica, one of the largest carriers in the world who has been recognised for its vision and execution capabilities in IoT.

As a result of the collaboration, Quectel has recently received certification of its LTE Cat NB2 (NB-IoT) module BC95-G from Telefónica, which includes subscription swap capabilities based on GSMA V3.2 standards.

These subscription swap capabilities are useful in Smart Metering (water, gas, electricity) and Smart Cities (waste management, parking, streetlight, pollution monitoring and more). For example, smart meters need to be deployed for 10-15 years and are often located in hard to reach locations, typically making the service cost of replacing subscriptions high. Additionally, subscription swap technology can help simplify the deployment, management and security implementation of future-proof smart meter devices.

Norbert Muhrer, Quectel's President and CSO, commented, "After close collaboration with Telefónica teams, our BC95-G module is reliable, well tested and proven in its capabilities for operating on Telefónica's NB-IoT network. Now customers can accelerate their IoT deployments worldwide."

The Telefónica-certified BC95-G is a high-performance NB-IoT module that supports multiple frequency bands of B1/B3/B5/B8/B20/B28 with extremely low power consumption. Designed for size sensitive applications and compatible with Quectel GSM/GPRS M95 and LPWA BC95 modules, it provides a flexible and scalable platform for new NB-IoT use cases.

Telefónica is currently working with customers on Smart Metering and Smart City projects to be deployed as a result of this achievement in Quectel BC95-G module.

## SCOTTISH POLICE DEPLOY TECH THAT EXTRACTS DATA FROM LOCKED SMARTPHONES


Designed by Freepik

Police Scotland has announced plans to establish "cyber kiosks" that will allow officers to scan locked smart devices for evidence.

The 41 new kiosks will be located in police stations across local policing divisions, where they will be operated by over 400 specially trained officers.

Each kiosk is essentially a desktop computer capable of performing data extraction, transfer, and analysis. The extraction devices are manufactured by Israeli company Cellebrite and are used around the world to retrieve data from cell phones, drones, and other types of digital technology.

Police Scotland said the Cellebrite devices will speed up their workflow and get smartphones that are found not to contain any information pertinent to an investigation back into their owners' hands more quickly.

"The technology allows specially trained officers to triage mobile devices to determine if they contain information that may be of value to a police investigation or incident. This will allow lines of inquiry to be progressed at a much earlier stage and devices that are not relevant to an investigation to be returned quicker," said Police Scotland.

Scottish police purchased the Cellebrite devices two years ago; however, legal concerns over how the technology may impact the public's right to privacy have delayed their deployment.

The Scottish Human Rights Commission and Privacy International have each said that the legal powers under which Police Scotland will operate the new technology are "not sufficiently clear, foreseeable or accessible."

Privacy International has expressed concerns over "the failure of Police Scotland to carry out impact assessments" in relation to the new technology. Deputy Chief Constable Malcolm Graham has said that the technology will only be used by the police where there is a "legal basis and where it is necessary, justified and proportionate" to an incident or crime under investigation.

Graham said: "Increases in the involvement of digital devices in investigations and the ever-expanding capabilities of these devices mean that demand on digital forensic examinations is higher than ever.

"Current limitations however, mean the devices of victims, witnesses and suspects can be taken for months at a time, even if it later transpires that there is no worthwhile evidence on them. By quickly identifying devices which do and do not contain evidence, we can minimise the intrusion on people's lives and provide a better service to the public."

## WEAK PASSWORDS CAUSED 30% OF RANSOMWARE INFECTIONS IN 2019

As one of the leading types of cyber-attacks, ransomware is expected to dominate cybercrime in 2020. According to PreciseSecurity.com research, weak passwords were one of the most common cybersecurity vulnerabilities in 2019, causing 30% of ransomware infections in 2019.

The recent PreciseSecurity.com research revealed that phishing scams caused more than 67% of ransomware infection globally during the last year. Another 36% of Mail Protection Service users reported ransomware attacks caused by the lack of cybersecurity training. Weak passwords were the third most common reason for ransomware infections globally in 2019.

The 30% share in the combined number of ransomware infections during the last years indicates a concerning level of password security awareness. The 2019 Google survey about beliefs and behaviours around online security showed that two in three individuals recycle the same password across multiple accounts. More than 50% admitted using one "favourite" password for the majority of the accounts. Only one-third of respondents knew how to define the password manager.

The 2019 Statista survey reveals that 64% of US respondents find stolen passwords as the most concerning issue about data privacy. However, such a high level of concern didn't affect their habits related to keeping track of login information. According to the findings, 43% of respondents reported that their primary method of keeping track of their most crucial login information was to write it down. Another 45% of respondents named memorising the login data as their primary method of tracking. At the same time, only 12% of US online users take advantage of password managers.

Using hard-to-guess passwords represent the first step in securing sensitive online information. However, according to the UK's National Cyber Security Centre 2019 survey, password re-use and weak passwords still represent a significant risk for companies and individuals all over the world.

The breach analysis indicated that 23.2 million victim accounts from all parts of the world used 123456 as a password. Another 7.8 million data breach victims chose a 12345678 password. More than 3.5 million people globally picked up the word "password" to protect access to their sensitive information.

## HIGH-TECH FIRMS PROVIDE BOOST TO CONSULTING INDUSTRY

Large technology companies have provided a massive boost to the consulting market as they expanded their use of services in the past couple of years, according to a new report.

In the technology, media and telecom (TMT) sector, high-tech companies such as Apple, Facebook and Google drove most of the business, with revenues rising 13.4% to US$4.8bn and growing by US$1bn in the past two years, according to a study by professional services analyst firm Source Global Research. By comparison, the global TMT consulting market grew at a slower pace, at 8.8% to US$12.9bn in 2018. According to the report, high-tech firms have increased their demands for consulting for risk and regulatory projects, especially when it comes to data privacy.

The General Data Protection Regulation (GDPR) was a "game changer" for consulting firms, it added, as it generated a lot of work when the regulations were enforced in May 2018, and that continues to be the case as companies want ongoing support to ensure compliance of products and services.

In addition, the report noted that other areas where high-tech firms have been looking to hire consultants for back office transformation projects, with a growing demand for managed services. Another task where they are looking for consultant support is for the shift to service-based technology offerings.

"The transition from one-off single-sale revenue structures to longer-term subscription sales models – often with lower upfront prices – is a complicated one that requires consulting firms to support through every stage of this transition," the report said.

The study also noted high-tech companies such as Apple and Google are also turning to consultants for support in shifting manufacturing operations out of China into locations such as India and South East Asia.

"Consultants are benefiting from high-tech companies seeking support to shift these complex manufacturing operations, and explore how to rethink and protect their wider supply chains," it concluded.

# INVIXIUM SHOWCASES BIOMETRICS INNOVATIONS AT INTERSEC 2020

Invixium, a manufacturer of modern, IP-based biometric solutions, showcased several new enhancements to the company's unique portfolio of biometric solutions for access control and workforce management applications at Intersec 2020 (stand S1-C12).


Featured enhancements on display include the faster and more responsive IXM WEB 2.1 biometrics software platform, new IXM MERGE 2 biometric device with an optical sensor for enhanced durability, and certified fingerprint and finger vein scanners integration solutions from Integrated Biometrics and Hitachi respectively. Also featured is Invixium's flagship TITAN; widely considered as the Most Advanced Biometric Solution Ever Engineered.

"It's high time that the entire biometric industry starts to focus on tangible benefits and solving real-life problems for customers rather than purely focusing on technology and features. It is due to this approach that Invixium continues to experience global acceptance of our unique biometric solutions for new and emerging access control and workforce management applications," said Shiraz Kapadia, CEO and President of Invixium. "We are continuing this pursuit of excellence here at Intersec 2020 with the public unveiling of our latest biometric all-in-one software IXM WEB along with our world-class products. The Invixium team of Biometric Solutions experts will be ready and prepared to listen to the most demanding access control and workforce management needs and offer executable solutions to increase productivity and enhance the security of your enterprise or industry."

Making its public debut at Intersec 2020, IXM WEB 2.1 Biometric Software Platform is 6X faster and more responsive and includes support for OSDP 2.0, TLS 1.2 encryption to ensure data protection and privacy. Additional new features include drill-down functionality for dashboard reports, advanced filter options for targeted reporting, and full integration of the new IXM MERGE 2.

MERGE 2 features an optical sensor for enhanced durability and construction via a solid metal backplate which acts as a heatsink for longer lasting operation. Other key features include Corning Gorilla Glass for exceptional protection for robust environments, multicolour LED status indicators, anti-shock and vandal protection, IPS capacitive touchscreen that can be used for PIN access, on-device enrolment and soft key inputs and PoE for fast and easy installation. MERGE 2 also provides support for various RFID card technologies ideal for a wide range of access control and workforce management applications.

Also featured in Invixium's stand at Intersec 2020 were the latest additions to the Invixium Certified Products (ICPs) portfolio; products made by other manufacturers that have been integrated into the IXM WEB biometric software ecosystem. New ICP additions include FBI certified single and multi-finger Columbo, Kojak and Five-O branded scanners from Integrated Biometrics and the H1 USB finger vein desktop scanner from Hitachi.

Invixium also showcased its best-in-breed IXM TITAN Multi-Biometric Device equipped with facial recognition as the primary biometric modality, and fingerprint or finger vein authentication as the secondary form of user authentication. TITAN consolidates features for access control, workforce management, video intercom and video surveillance into a single device for a diverse host of applications with extreme efficiency and convenience.

# RETAILERS DEPLOYING NEW OMNICHANNEL FUNCTIONALITY WITH RFID

Technology company Checkpoint has released a new version of its HALO Internet of Things (IoT) software platform to support in-store fulfilment of omnichannel orders, including a feature known as "task management" and updated omnichannel-based functionality in an app used in stores. The software automatically routes online orders to the appropriate stores based on inventory availability, and store associates can automatically receive and then fulfil "buy online pickup in store" (BOPIS) orders, as well as ship-from-store purchases.

*To be continued on page 21*

Companies such as Spanish fashion brand Desigual are using the latest version of HALO to streamline their omnichannel services.

Checkpoint makes RF- and RFID-based loss-prevention and merchandise-visibility solutions. Retailers can use the company's system to gain inventory data and reduce the incidence of theft. The firm released its HALO solution in 2018 to provide UHF RFID-based visibility into store inventory, as well as data regarding the location and status of goods at manufacturing sites and distribution centres, according to Carl Rysdon, Checkpoint's VP of RFID solutions.

Use cases include tracking goods from the point of manufacture to the store, or from DC to store, or in the store itself. At the store level, everything the associate does can be accomplished via an app on an iOS- or Android-based device paired with his or her choice of RFID reader. Rysdon calls it the only platform with this widescale functionality in the industry.

As omnichannel sales become the norm, however, retailers are increasingly using RFID technology and solutions such as HALO to enable order fulfilments. For instance, some retailers have been using HALO's cloud-based software and app to look up the in-store availability of items, in order to find them within a store using an RFID reader, and thereby speed up the process of in-store fulfilment.

"We help our clients deliver on their omnichannel promise to their customers," Rysdon says. The company thus developed an omnichannel functionality that enables retailers to integrate RFID data into their existing order-management system, thereby streamlining the order and fulfilment process.

When a customer places an order, the HALO software automatically determines which stores have the products being purchased, in the most appropriate locations. It then forwards that data to the store. A task is automatically generated for store associates, which they can view on their HALO app in the form of a shopping basket. The employees can use the app on their phone, which is paired with an off-the-shelf UHF RFID reader via a Bluetooth connection. They can use the app and the handheld to perform inventory-related tasks in the store, including filling orders.

With HALO's new Item Locator feature on the app, sales associates can use their handheld reader to guide them to a particular item. They can simply select the prompt to locate that product, then use the reader similarly to a Geiger counter. While packing the order, workers scan the item with the RFID handheld, select an item on the touch screen and mark it as "done".

*Designed by Bakar015 / Freepik*

Alternatively, they can scan a barcode on the product's label. Retailer managers can view this data to understand the status of each shipment, and to receive inventory level updates. In that way, they know when orders are not fulfilled and when problems may arise, as well as monitor inventory levels at each store.

This omnichannel functionality, paired with the task-management feature, ensures that employees are more productive, Rysdon explains, since order fulfilment can be accomplished easily without workers spending time locating goods and then manually updating the order status in the management software. Thus, he says, they are "able to focus more on customer-facing activity".

Inventory data from a store's enterprise resource planning system may not be accurate or up to date. Therefore, an order may still be sent to a store, even if all items purchased may not be available there. That can lead to order rejection, delays in multiple shipments. However, HALO Task Manager distributes orders based on inventory availability. This drives several key performance indicators for retailers. For one thing, Rysdon says, because the inventory data is updated with each order, and because the HALO system routes orders specifically to stores with available inventory, a higher fulfilment success rate results.

That leads to time savings, greater fulfilment success rates and lower shipping costs, Rysdon explains, since a company can send out items from fewer locations. Additionally, managers can track the units per hour for pick times or shipping tasks, and they can identify when there may be a problem that is affecting efficiency.

The Task Management functionality has been expanded to enable users to create non-RFID or inventory-management-based projects for staff members, Rysdon notes. For instance, if management requires personnel to accomplish a specific job, such as cleaning a sales area, that can be shared with the staff via the HALO app.

Existing HALO customers have access to the added functionality. Desigual has already launched the solution, while several other retailers are in the pilot stage of the latest HALO version. Because HALO is provided as a software-as-a service, Checkpoint can continue to add functionality for a retailer or brand, as well as enabling that company to select the features it needs. "We have a roadmap to add functionality to create more ways for customers to benefit from RFID," Rysdon states.

## 14 ENGLISH PREMIER LEAGUE CLUBS HAVE DECIDED FOR "PANOMERA®" FROM DALLMEIER ELECTRONIC"

Like many national football leagues, the teams of the English Premier League also suffer from unacceptable incidents such as lighting of pyrotechnics and throwing projectiles, hate crime and vandalism. This is why as early as 2013 the managers at Everton F.C. opted for a patented video security solution from the German video technology company Dallmeier. Today, 14 of 20 clubs of the 2019–20 Premier League season have implemented Dallmeier "Panomera®" multifocal sensor systems – including Arsenal, Chelsea, Liverpool and Manchester United.

Many teams in the top flight of English football are also involved in the Champions League and Europa League, so it is also extremely important for them to satisfy the safety regulations imposed internationally by UEFA and similar bodies. For this purpose, Dallmeier solutions enable high-resolution capture of expansive areas, such as the stands, with a minimum number of camera systems. With Panomera® cameras, multiple operators have the capability to zoom in on suspicious activities independently of each other, while the system continues recording the entire scene. This combination of the advantages of PTZ and megapixel cameras, an optimum overview of the situation is obtained, which can also be searched in the required minimum resolution at any time afterwards. This enables the clubs to achieve continuity of video evidence, get instant ID of people and events, and so reduce potential penalty payments.

Besides the court usability of video recordings, the "minimum resolution density" is also important for video analysis applications. As stated so succinctly by the rule "quality in, quality out", of course the quality of the results of analysis – for example in "crowd analyses" for people counting on stands, for "hostile vehicle mitigation" or to detect intrusion in sterile areas – can only ever be as good as the quality of the image, and accordingly the quality of the input data. With Dallmeier solutions, as early as the planning stage customers can precisely specify the pixel density values defined according to DIN EN 62676-4 for each region of the area captured – depending on whether for example at least 62.5 px/m is required for AI-based object classification, or 125 or even 250 px/m is required to guarantee that recordings of persons will be usable in court.

"Throughout our selection procedure, the Panomera® cameras from Dallmeier were able to deliver images of the highest quality time after time, not only in normal daylight conditions, but also under weaker floodlighting, that is to say not only live but also in the recording with the highest resolution quality in all regions of the images. Moreover, with the Panomera® cameras we can capture large expanses, the entire area of the stands, for example, with just a small number of systems. Ultimately, these considerations were the critical factor in our decision to award Dallmeier the contract for video security at Goodison Park", says David Lewis, Head of Security and Stadium Safety for Everton F.C.

The innovative 3D planning approach by Dallmeier provides stadium operators with the ability to place each individual camera with the highest precision in advance through the use of a "digital twin". Thus, even the planning contributes to a reduction of total costs. At the same time, the in-house planning team uses it to manage any difficulties such as visual obstacles (e.g. a video cube) or subsequent structural changes. This ensures that there are no "cost traps" for the customers, and that compliance with all requirements is guaranteed without exception when the system is implemented.

## SENSTAR APPOINTS FABIEN HAUBERT AS MANAGING DIRECTOR

Senstar, a market-leading provider of video management and perimeter intrusion detection technologies, is pleased to announce the appointment of Fabien Haubert as Managing Director. Haubert will help Senstar strengthen its position as a global leader of physical security solutions with a focus on addressing the specific needs of key vertical markets.

“Senstar is in an exciting period of momentum and growth and I am looking forward to working with our unmatched team of security experts to build on this success,” said Haubert. “As the security landscape changes, we are committed to evolving our offerings to meet and exceed new challenges with comprehensive, integrated solutions.”

*To be continued on page 23*

Haubert joined Senstar in 2018 as Vice President, Sales – EMEA, where he has streamlined sales and support organisations and led a significant growth in revenue in the region. Prior to Senstar, Haubert worked in senior roles with several companies in the areas of video management, IP video surveillance, intrusion detection, access control, and system integration. Haubert has a technical background with an Master of Science degree in Telecom Engineering, as well as a Master of Management and Strategy of International Business degree. He speaks French, English, Spanish, and Italian, and has a working knowledge of Dutch.

Haubert will be relocating from France to Senstar's Ottawa, Canada headquarters in June 2020.

## PRIVAFY CLAIMS 'FUNDAMENTALLY NEW' APPROACH TO MOBILE DATA SECURITY

Former Verizon and NXP Semiconductors executives have launched Privafy, a cloud-native, security-as-a-service application to protect data in motion.

The company says it offers a "fundamentally new" approach to data security that protects organisations against modern mobile threats while disrupting the cost associated with what can be complex, archaic network solutions.

"Data has never been less secure," said Privafy co-founder and CEO Guru Pai (pictured above). "Solutions developed by the networking industry to protect data are rapidly becoming obsolete for today's cloud-and mobile-based workloads.

"Also, technologies such as SD-WAN and cloud-based point solutions focus more on cost reductions, but don't address the underlying security vulnerabilities to sufficiently protect internet-reliant businesses. Privafy was purpose-built to secure data in today's modern world. We have democratised internet security to protect data in a way that is easier to deploy and far more economical for any-sized enterprise, regardless of where or how it works."

*Designed by starline / Freepik*

Pai cited a Gartner research document, The future of network security is in the cloud, which noted that digital business transformation inverts network and security service design patterns, shifting the focus to the identity of the user and/or device, and not the datacentre. The report said the idea of the legacy datacentre as the hub of business network and network security architecture was obsolete and had become "an inhibitor to the needs of digital business".

Privafy's core application is designed to secure data in motion as it moves across locations, clouds, mobile and the internet of things (IoT). The application integrates the functionality of encryption systems and VPNs, firewalls, distributed denial of service (DDoS) protection, intrusion detection and prevention systems (IDS and IPS), data loss prevention and deep content inspection technology.

Functionality includes a proprietary absolute encryption schema that defends against man-in-the-middle or unauthorised snooping attacks, and endpoint identity protection that protects against endpoint cloning.

Proprietary technology also protects remote workforces on iOS, Android, Windows, macOS and Linux, enabling support for all the environments in which an enterprise operates, including headquarters, branch offices and global sites, mobile and personal computers, private and public clouds, software-as-a-service (SaaS) applications such as Salesforce, Slack and Dropbox, and the IoT.

## MICROSOFT EXPOSES 250 MILLION CALL CENTRE RECORDS IN PRIVACY SNAFU

Microsoft briefly exposed call centre data on almost 250 million customers via several unsecured cloud servers late last year, according to researchers. Bob Diachenko spotted the major privacy snafu a day after databases across five Elasticsearch servers were indexed by the BinaryEdge search engine on December 28.

Each contained a seemingly identical trove of Microsoft Customer Service and Support (CSS) records spanning a 14-year period. The records included phone conversations between service agents and customers dating back to 2005, all password-free and completely unprotected, according to Comparitech.

Most personally identifiable information (PII) was redacted from the records, but "many" apparently contained customer email and IP addresses, support agent emails and internal notes and descriptions of CSS cases.

This presented not just a phishing risk but a valuable collection of data for tech support scammers who impersonate call centre agents from Microsoft and other companies to install malware on victim machines and steal financial data.

"With detailed logs and case information in hand, scammers stand a better chance of succeeding against their targets," explained Comparitech's Paul Bischoff.

"If scammers obtained the data before it was secured, they could exploit it by impersonating a real Microsoft employee and referring to a real case number. From there, they could phish for sensitive information or hijack user devices."

However, Microsoft was praised for acting swiftly to lock down the exposed servers.

After being informed by Diachenko on December 29, the firm had secured all data by December 31.

Microsoft is just the latest in a long line of companies that have exposed sensitive consumer data through cloud misconfigurations. These include Choice Hotels, Honda North America, Adobe and Dow Jones.

Sometimes the leaks come from suspected cyber-criminals. Back in December, over one billion email and password combos were exposed via an unsecured Elasticsearch database, with many collected from a previous 2017 breach.

## SEMTECH RELEASES NEW LORA® SMART HOME DEVICE FOR IOT APPLICATIONS

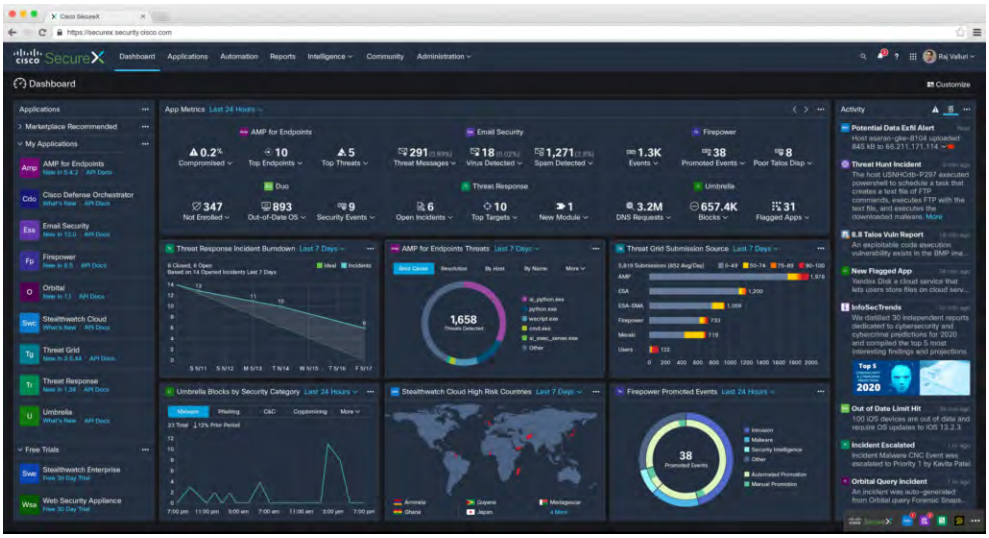
Semtech Corporation announced the launch of LoRa® Smart Home, a device designed for LPWAN based smart home, community and consumer applications. The transceiver provides low power, broad coverage for indoor and neighbourhood area IoT devices connecting to sensors and actuators for safety, environmental and convenience use cases.

"With its simple and flexible network architecture, Semtech's new LoRa® Smart Home device offers a unique opportunity to accelerate the consumer adoption of smart home connected solutions. As an end-to-end solution, or as a complement to Wi-Fi, LoRa Smart Home broadens smart home solutions by enabling connectivity for low cost and battery powered end points both indoors and outdoors," said Pedro Pachuca, Director of IoT Wireless in Semtech's Wireless and Sensing Products Group.

"The new LoRa Smart Home device provides a flexible and cost effective solution for low latency smart home applications, including smart key locks and lighting, enabling low cost network extension and providing a bridge to the many LoRaWAN®-based B2B and B2C solutions available in the IoT market today."

The new transceiver is intended for battery-powered sensors with multi-year operation. It features 600nA of sleep current and 4.6 mA of active receive current consumption. With support for LoRa modulation for low power LAN use cases and (G)FSK modulation for legacy use cases, this device is compatible with existing LoRaWAN-based networks and supports proprietary protocols. Continuous frequency coverage from 150 MHz to 960 MHz allows the support of all major sub-GHz ISM bands around the world.

# CISCO LAUNCHES SECUREX PLATFORM FOR INTEGRATED SECURITY




Nearly a decade after first introducing its SecureX framework, Cisco has expanded the strategy with a full-fledged platform for its integrated security products.

At RSA Conference 2020 Monday, the networking giant unveiled the Cisco SecureX platform, which aims to connect integrated Cisco security products along with customers' infrastructure for a unified experience.

Cisco first introduced the SecureX framework at RSA Conference 2011; the network-centric security framework was designed to integrate Cisco products to streamline policy enforcement and provide enterprises with contextual awareness regarding devices, users and potential threats.

The Cisco SecureX platform builds on that strategy by giving enterprises a central point that connects to the vendor's integrated security portfolio and the customers' environments. Jeff Reed, senior vice president of Cisco's Security Business Group, said the cloud-native platform offer several core capabilities.

"First, it enables visibility across the breadth of our security products from a single place," he said. "Second, we're able to automate remediation, such as blocking suspicious IP addresses, hashes or domains."

In addition, Cisco SecureX provides a new feature the vendors described as "managed threat hunting," courtesy of Cisco Talos' team of threat analysts. "This is essentially our Talos researchers being able to do managed threat hunting within the customers' environments, where they're looking for new campaigns and IOCs [indicators of compromise] and bringing the intelligence back to the customers," Reed said.

While the SecureX platform is an expansion of the previous framework strategy, Reed said Cisco Threat Response, a tool for security operations centre analysts, was one of the key "bricks of the foundation" for the platform. A primary goal of SecureX, Reed said, is to give enterprise security professionals a better way to view, react and respond to both alerts and full-blown incidents.

"We're trying to help simplify the experience, reduce the amount of errors and make it easier for multiple individuals to work on a single issue and provide better visibility, faster time to remediation and more efficient utilisation of resources," he said.

The SecureX platform will be included with every Cisco security product license at no additional cost. In addition to Cisco's own product portfolio, the SecureX platform will be able to integrate with third-party products and services. "Part of the automation capability set for SecureX is out-of-the box integrations with systems like ServiceNow, for example," Reed said.

He added that Cisco is currently working with other partners to bring third-party products to the platform, which the company plans to announce when SecureX officially launches at the Cisco Live conference in June.

Jon Oltsik, senior principal analyst at Enterprise Strategy Group, said Cisco is making good on its strategy to integrate its product portfolio.

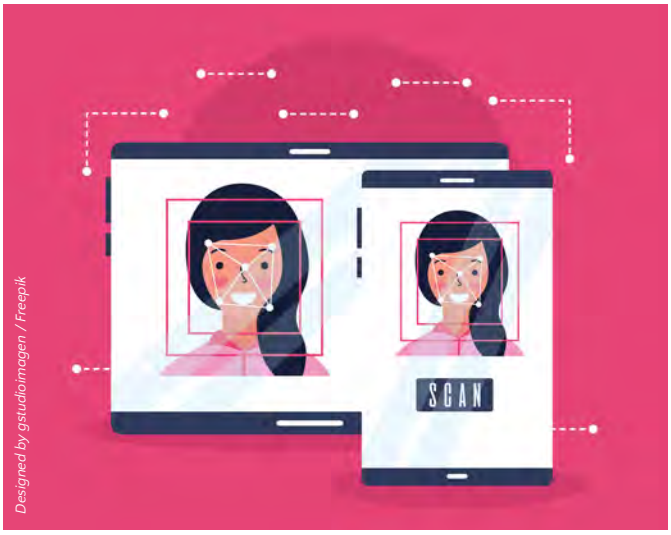
"In 2011, it was more of a vision, but Cisco had a lot to do just to integrate Cisco and Sourcefire products. This is much further advanced with a common interface, cloud backend, etc.," Oltsik said via email. "This is the direction the industry has to go. The entire cybersecurity technology infrastructure must be tightly integrated to share data and intelligence, alerts, analytics and action. SecureX is the first step toward this end, and Cisco has an aggressive roadmap behind its initial release."

# NEC TO PROVIDE FACIAL RECOGNITION TECHNOLOGY FOR MITSUI FUDOSAN HOTELS

NEC Corporation, a leader in the integration of IT and network technologies, announced it will provide a "Smart Hospitality Service" utilising facial recognition technology for "Sequence", a newly developed hotel brand by Mitsui Fudosan and Mitsui Fudosan Hotel Management.

NEC's "Smart Hospitality Service" helps to ensure safe, secure, and efficient stays by utilising facial recognition technology for a wide range of services, including check-in, entering rooms and entertainment facilities, and making cashless payments. Each of these services helps to improve the convenience of hotels, to relieve stress, and to promote a more comfortable experience and stay.

The service links pre-registered facial information with reservation information in advance, allowing guests to complete check-in smoothly and simply with a tablet device equipped with facial recognition. Also, when entering their rooms, guests can unlock the door with just facial recognition, thereby eliminating the need for keys and the concern of having to replace them if they are lost or stolen.



Designed by gstudioimagen / Freepik

Facial recognition is at the core of NEC's portfolio of biometric identification technologies, "Bio-IDiom," and utilises NEC's facial recognition AI engine "NeoFace," which has the world's No.1 certification accuracy.

This service will be available for registered guests who agree to the use of facial recognition. Facial information will not be saved nor used for verification without confirming a guest's consent.

Hotels with Face Recognition:
- Sequence, MIYASHITA PARK (June 2020)
- Sequence, KYOTO GOJO (July 2020)
- Sequence | SUIDOBASHI (provisional name, expected to open in the fall of 2020)

*Sequence, MIYASHITA PARK only provides facial recognition at check-in.

In the future, NEC aims to expand the range of its "Smart Hospitality Service," enabling guests to go sightseeing directly from the airport by checking-in through facial recognition and having baggage delivered to the hotel.

NEC's "Smart Hospitality Service" allows information on the status of people, things, and processes to be shared across the entire value chain, helping to realise "NEC Value Chain Innovation."

# 128 TECHNOLOGY'S SOLUTION TO BE OFFERED BY SOFTBANK CORP

128 Technology, the leader in Session Smart™ Networking, announced that Japan-based SoftBank Corp. ("SoftBank") has selected the 128T Networking Platform to offer its enterprise customers a tunnel-free, managed SD-WAN solution that greatly enhances their network performance and security. The service is being branded as "SD-WAN Type X" and represents a leap in innovation for IP network service delivery. SoftBank is a carrier that provides ISP and network services in addition to mobile communications.

Many of SoftBank's enterprise customers are looking for networking solutions that will enhance their connectivity with cloud-based applications that drive their business forward. 128 Technology's solution will enable SoftBank to provide its telecommunications and technology enterprise customers with a tunnel-free SD-WAN solution that offers faster access to the cloud and better connectivity with branch locations. By eliminating tunnels, the 128T Networking Platform and

*To be continued on page 27*

Session Smart Router™ will more effectively route network traffic to better pathways when there is network congestion, increasing both connectivity and bandwidth.

Additionally, SoftBank's "SD-WAN Type X" offering reduces complexity and operations costs by eliminating firewalls and VPNs and by cutting cloud rental costs.

The 128T Networking Platform also is designed around a "Zero-Trust" security model, so enterprise customers that are transferring large amounts of sensitive data over their network can rest assured that it will remain protected, reducing the risk of security breaches.

"We have a fundamental 'Beyond Carrier' strategy and aim to achieve sustainable growth by expanding beyond the traditional framework of telecommunications carriers by collaborating with leading companies with advanced technologies. More enterprises are not only interested in deploying SD-WAN to keep pace with digital innovation; they also seek a partner with the expertise to help them deploy their SD-WAN solution most effectively," said Kunihiro Fujinaga, Senior Vice President and Head of Enterprise Product & Business Strategy at SoftBank.

"Our new service 'SD-WAN Type X' consisting of 128 Technology's solution is designed to help enterprises leverage their network to give users faster and more reliable access to the cloud-based applications that form the backbone of their business."

"By utilising our SD-WAN solution, SoftBank's enterprise customers will be able to connect users with great experiences by efficiently delivering applications and resources that drive today's businesses forward," said Tim Ziemer, Vice President of Worldwide Sales & Business Development at 128 Technology. "We're very excited to expand our presence in Japan and look forward to providing agile WAN connectivity to SoftBank customers that delivers enhanced security, performance and agility."

## POONSUB CAN PARTNERS WITH NTT LTD. TO DRIVE DIGITAL TRANSFORMATION STRATEGY AND BUSINESS GROWTH

NTT Ltd., the world-leading global technology and business solutions leader, announced the successful implementation of an integrated digital automation platform for Poonsub Can, one of Thailand's leading metal packaging companies. The implementation, part of Poonsub Can's Digital 4.0 plans, aims to boost business productivity and operational capacity with a robust digital infrastructure that better responds to customers' evolving needs.

Over the past year, NTT Ltd. in Thailand led the successful implementation of SAP S/4HANA in partnership with NTT Data Thailand and Netizen Co, a third-party technology vendor. With strong capabilities in systems integration, NTT Ltd. in Thailand provided technical knowledge and strategic counsel that includes a review of existing IT systems, recommendations on technology enablement and innovative ways to gain business agility through intelligent automation.

Powered by artificial intelligence and deep analytics, the new IT systems will improve service gaps and speed up response time to customers' queries, ensuring that they are attended to in a timely manner. Quality control is also optimised with built-in traceability functions, eliminating human error while elevating production standards and overall productivity. With productivity gains in ASEAN's manufacturing sector set to double from $670 billion by 2028, refreshing the legacy system can advance business growth by future- proofing Poonsub Can's business operations, laying a new foundation for growth.

"It's an exciting time for Poonsub Can as we embark on this new digital journey with our enhanced technological capabilities. Through our close partnership with NTT Ltd., we have identified new opportunities that will spur continuous business growth and drive innovation, enabling us to better provide more value to our customers. As Thailand charges forward with its digital transformation masterplan, it is imperative for manufacturers to embrace technology and deploy smart solutions that drives industry growth and foster greater economic progress for the nation." Said Viboon Trakulpoonsub, Managing Director, Poonsub Can Co., Ltd.

"Innovation is at the core of our business, and the implementation of SAP S/4HANA is another prime example of how NTT Ltd. delivers intelligent solutions that addresses our clients' transformational challenges. Combining Thailand's ambitious digital goals with Poonsub Can's objectives, we exchanged global best practices in the manufacturing sector and identified actionable steps toward implementing SAP S/4HANA, so that Poonsub Can is empowered with the right foundation to optimise operations and improve customer satisfaction, laying ground for new business opportunities." Said Sutas Kondumrongkiat, CEO, Thailand for NTT Ltd.

## SK TELECOM CLAIMS STANDALONE 5G DATA SESSION IS WORLD'S FIRST

In a move that simultaneously establishes the country as a world leader in 5G and places itself as top dog in a hugely competitive marketplace, Korean telco SK Telecom has revealed that it has successfully accomplished the world's first standalone 5G data session on its multi-supplier commercial 5G network.

The move, described as a major breakthrough for the 5G arena, will allow SK Telecom to launch the world's first 5G standalone service in the first half of 2020.

The standalone 5G data call took place on 16 January 2020 in Busan, the second largest city in Korea, using SK Telecom's commercial 5G network deployed in that region.

The company applied standalone New Radio (NR) software to its existing non-standalone 5G base stations, and completed multi-supplier interoperability between network equipment of Ericsson and Samsung. SK Telecom has also applied key 5G technologies such as network slicing and mobile edge computing (MEC) to its standalone 5G network. Network slicing is being highlighted as an essential technology for providing optimal support for different types of 5G services by partitioning a single physical network into multiple virtual mobile networks.

MEC is designed to minimise latency by providing a shortcut for data transmission through installation of small-scale data centre at 5G base station or router. MEC can improve the performance of ultra-low latency 5G services such as cloud gaming, smart factory and autonomous driving.

Earlier in January 2020, SK Telecom unveiled the Global MEC Task Force, in cooperation with Singtel, Globe, Taiwan Mobile and PCCW Global. The companies are uniting to make joint efforts to develop MEC technologies and services, setting international MEC standards and building an interoperable MEC platform. "With the successful standalone 5G data call on our multi-vendor commercial 5G network, we are now standing on the threshold of launching standalone 5G service, a key enabler of revolutionary changes and innovations in all industries," said Park Jong-kwan, vice-president and head of 5GX Labs of SK Telecom. "SK Telecom will offer the best 5G networks and services to realise a whole new level of customer experience in the 5G era."

Standalone 5G networks have been tested worldwide, but Asia stands out as a hotspot for the field. In December 2019, China Mobile in Hong Kong announced that it had successfully accomplished a 5G standalone network test and completed the first voice over NR call in Hong Kong.

In the same month, Swedish comms tech giant Ericsson revealed Asian projects that could create new 5G services for consumers and enterprise customers with emerging technologies, among which was the successful completion of 5G standalone voice services.

## MOU SIGNED TO LAUNCH DIGITAL ECONOMY PLATFORM DIGITISING MALAYSIA AND ITS TRADE PARTNERS

Malaysian Technology Development Corporation (MTDC) and Ireland's semi-governmental World Logistics Council Limited (WLC) signed a Memorandum of Understanding (MoU) to deploy the organisation's Digital Economy Platform, the Multi-Dimensional Digital Economy Application System (MDDEAS®).

Through this MoU, MTDC and WLC will promote the deployment of MDDEAS®, in cooperation with the world's largest technology firms, which will digitally connect businesses in Malaysia with their global trade partners and trigger enhanced efficiency and security of trade, with Malaysia serving as a benchmark for the world. MDDEAS® is built based on a catalogue of product and process innovations that leverage the latest technologies, including Artificial Intelligence (AI), Big Data Analytics, and Blockchain, among others, to de-risk commerce, reduce costs, and create greater access to finance and insurance services globally.

Dato' Norhalim Yunus, MTDC Chief Executive Officer and Captain Samuel Salloum, WLC Chairman and Chief Executive Officer signed the MoU, which was witnessed by Tan Sri Abdul Rahman Mamat, MTDC Chairman. MTDC Chairman Tan Sri Abdul Rahman said the platform will assist Malaysia connect local businesses to foreign partners and expand into global markets. "This collaboration marks another milestone for the companies in MTDC's ecosystem as MDDEAS® can

*To be continued on page 29*

better connect our local SMEs to global markets through a seamless borderless digital marketplace and create tremendous market expansion opportunities. MTDC in its role as the strategic enabler for I4.0 for local SMEs will identify those SMEs who can benefit from the MDDEAS® tools. It is important to do all this in a new digital format."

The MoU closely aligns with the Government's Shared Prosperity Vision 2030 (SPV 2030) which focuses on high-impact industries such as aerospace, digital economy and high-tech farming.

WLC Chairman Captain Samuel Salloum said that MDDEAS® offers "thousands" of on-demand applications that enable businesses to synchronise their logistics, insurance, financial and commerce systems with other businesses worldwide to establish a new "21st-century efficiency level".

The WLC aims to enable MDDEAS® users to tap into the world's business-to-business (B2B) market, currently valued at USD 150 trillion, and deliver a new USD 20.5 trillion digital services marketplace, more than ten times the size of current oil and gold production combined.

Captain Salloum exclaimed, "We are pleased this initiative was pioneered by Johor Corporation, whose vision and 10 years of R&D has contributed to the Digital Economy being adopted as a key G20 Leaders' policy directive and amassing more than 150 countries, 26 IGOs/ NGOs and prominent firms to deploy the platform. With the MoU signing, MTDC will apply its technical resources and strategic alliances to commercialise the platform benefiting Malaysia, ASEAN and their trade partners worldwide."

The advantage of MDDEAS® over existing platforms is that it captures high quality data that is automatically cross-checked and validated by multiple organisations within the system, he said. "Through a unique balanced governance and deployment structure, the platform offsets geopolitical, monopolistic and data privacy concerns related to trade and trade data which are of national security importance."

Dato' Norhalim Yunus, MTDC Chief Executive Officer elaborated, "We are delighted to be part of this global initiative that will digitise the value chains of Malaysia and its trade partners. This collaboration marks another milestone for MTDC as we will identify those companies who will benefit from the world digital market."

## SYNOPSYS AND FINASTRA PARTNER TO SECURE FINANCIAL SERVICES APP ECOSYSTEM

Synopsys, Inc. and Finastra announced a partnership establishing an application security validation program for FusionFabric.cloud, Finastra's open platform for developing, deploying and consuming financial applications. The program, powered by the Synopsys Software Integrity Group, ensures that all applications offered via the FusionFabric.cloud FusionStore have passed thorough vigorous security testing assessments.

"By partnering with Synopsys on our application validation program, we're creating a win-win solution for financial institutions and Fintech developers," said Nir Valtman, head of product and data security at Finastra. "Financial institutions can streamline the onboarding process for new applications and bring innovation to market faster, and Fintech providers get third-party validation from an industry-leading application security company."

FusionFabric.cloud is a scalable, open, and collaborative development platform that enables Fintech providers to create and bring applications to market faster.

Synopsys will help validate the security posture of all applications onboarded to FusionFabric.cloud, using solutions that include static application security testing, software composition analysis, penetration testing, and code reviews.

"In today's dynamic threat landscape, security is a requisite component of innovation, especially in the Fintech space," said Steve McDonald, co-general manager of the Synopsys Software Integrity Group. "The application validation program leverages Synopsys' security testing technology and expertise to ensure that applications published on the FusionFabric.cloud platform are designed, developed, and deployed with the highest standards for security. The net result is that Fintech providers can focus on delivering innovative solutions rapidly, and their financial services customers can rely on them with confidence."

Early adopters of the platform, who have already completed the application validation program, include Allied Payment Network and Monotto.

"The FusionFabric.cloud platform has provided us with inroads to Finastra's client base, and has driven demand for the RoboSave app, our automated savings tool," said Christian Ruppe, CEO and Co-Founder, Monotto. "By going through Synopsys' rigorous validation process before being made available on the FusionStore, banks have peace of mind that RoboSave meets the highest standards for security."

# INTERPOL UNCOVERS CYBER CRIME OPERATION IN INDONESIA

An Interpol-coordinated cyber operation against a strain of malware targeting e-commerce websites has identified hundreds of compromised websites and led to the arrest of three individuals who were allegedly running the malicious campaign from Indonesia.

The malware, known as a JavaScript-sniffer, the online equivalent of a traditional card skimmer, targets online shopping websites. When a website is infected, the malware steals the customers' payment card details and personal data such as names, addresses and phone numbers, sending the information to command and control (C2) servers controlled by the cyber criminals.

Dubbed Operation Night Fury, the operation was conducted with the support of cyber security firm Group-IB, which provided data on the reach of the malware that has infected websites in several countries including Indonesia, Australia, UK, US, Germany and Brazil. Group-IB also supported the investigation with digital forensics expertise to help identify the suspects.

The Interpol's ASEAN Cyber Capability Desk has since disseminated cyber activity reports to the affected countries, highlighting the threat to support their national investigations, including information on C2 servers and infected websites located in six countries in the Association of Southeast Asian Nations (ASEAN) region.

At the request of Indonesian police, Interpol provided technical and operational support that resulted in the arrest of three individuals suspected of commanding the C2 servers in the country. The investigation revealed the suspects were using the stolen payment card details to purchase electronic goods and other luxury items, then reselling them for a profit. They have been charged with the theft of electronic data, which carries up to a 10-year jail sentence in accordance with Indonesia's criminal code.

"Strong and effective partnerships between police and the cyber security industry are essential to ensure law enforcement worldwide has access to the information they need to address the scale and complexity of today's cyber threat landscape," said Craig Jones, Interpol's director of cybercrime.

"This successful operation is just one example of how law enforcement is adapting and applying new technologies to aid investigations, and ultimately reduce the global impact of cybercrime," he added.

In Singapore, local authorities identified and took down two of the C2 servers. Investigations in other ASEAN countries are ongoing, with the Interpol continuing to support police

in locating C2 servers and infected websites, and identifying the cyber criminals involved.

The perpetrators behind the latest attack involving the use of JavaScript-sniffers were not new to the world of cybercrime. To access servers that collected stolen data and control their malware, they used virtual private network (VPN) connections to mask their real location and identity. To pay for hosting services and buy new domains, they only used stolen cards, according to Group-IB.

"Thanks to the Indonesian police and Interpol's prompt actions, Operation Night Fury became the first successful multi-jurisdictional operation against the operators of JavaScript-sniffers in the Asia-Pacific region," said Vesta Matveeva, head of Group-IB's cyber investigations team in the region.

"It is a great example of coordinated cross-border anti-cybercrime effort, and we are proud that our threat intelligence and digital forensics expertise helped to establish the suspects. We hope this will set a precedent for law enforcement in other jurisdiction too," she added.

In a separate incident that took place under a year ago, the payment card information belonging to thousands of customers of Singapore banks was believed to have been compromised by a JavaScript-sniffer and put up for sale on the dark web.

During their analysis of underground card shops, Group-IB's threat hunting team discovered a spike in the sale of raw data of 4,166 compromised payment cards – including CVV, card number and expiration date – issued by Singapore banks.

Group-IB said the data was uploaded in April 2019, and that the spike took place on 1 April when a database containing data on 1,726 compromised cards was put up. The mean figure from January to August 2019 was 2,379 cards per month.

## TELTRONIC INSTALLS NEPAL'S FIRST TETRA SYSTEM IN KATHMANDU AIRPORT

Teltronic has installed Nepal's first TETRA network in Tribhuvan International Airport, Kathmandu, providing users and security teams with a comprehensive critical communications solution.


Designed by rawpixel.com / Freepik

The Spanish company has deployed its NEBULA TETRA infrastructure, which has replaced the airport's existing analogue radio, meeting the main requirements defined by airport authorities: higher security standards, built in scalability to allow additional users and the integration of other airport technology. The chosen offers flexibility for varied work groups, with the highest level of encryption to ensure security, and robust Sepura CSC20 radios which can be connected to the Wi-Fi service, enabling integration with existing airport data and control systems.

In this way, the entire site is covered by the new TETRA network, ensuring that airport workers and security personnel are in constant communication with the control rooms.

Additionally, one of the main advantages of the solution provided by Teltronic and Sepura is the fact that radios' high transmitter power extends coverage where lower power radios struggle. This is a key feature of the security capability for the airport, ensuring that users based in remote locations, underground facilities or within large building are kept in touch with the control room.

Tribhuvan International Airport serves as an international hub for over 30 domestic and international airlines and saw over 7 million passengers passing through in 2018, with future increases expected. Situated in Kathmandu Valley, the airport features a passenger terminal, plus extensive outdoor maintenance facilities, parking areas and other large buildings.

The new TETRA network allows for the smooth movement of passengers through the airport by increasing co-operation between different work groups - including maintenance units, cleaning teams, airline staff, airside crews, security and emergency responders. Passengers benefit from a smoother experience with fewer delays, whilst the airport and airlines both benefit from more efficient working practises whilst fines and compensation for late running are minimised.

## SAMSUNG INTRODUCES BEST-IN-CLASS DATA SECURITY CHIP SOLUTION FOR MOBILE DEVICES

Samsung Electronics Co., Ltd., a world leader in advanced semiconductor technology, today introduced a Common Criteria Evaluation Assurance Level (CC EAL) 5+ certified Secure Element (SE) turnkey solution for mobile devices. The new SE offers a strong security solution, consisting of a security chip (S3K250AF) and optimised software, that fully guards private data on an isolated data storage.

"Strong security measures have become a crucial feature in today's smart devices as they evolve into essential tools that hold the key to our personal data connected to various services such as the cloud and financial transactions," said Dongho Shin, senior vice president of System LSI marketing at Samsung Electronics. "Samsung has a long and proven history in security solutions such as smart card ICs, IoT processors and other semiconductor products that require robust security. Our new turnkey SE solution for mobile devices will not only keep user data safer on the go but also enable new mobile applications that will broaden and enrich our everyday lives."

From checking emails and making online-payments to replacing house keys and airplane tickets, smart devices continue to offer more applications that enforce stronger security requirements. Samsung's new turnkey solution is a dedicated tamper-resistant strongbox that securely stores users' confidential and cryptographic data such as pin numbers, passwords and even crypto-currency credentials separate from the typical mobile memory such as embedded Universal Flash Storage (eUFS).

The S3K250AF-based SE combines a microcontroller, advanced hardware-level protection and an optimised secure OS. With a CC EAL 5+ certified-hardware, the highest level received by a mobile component, and dedicated protection software, the solution ensures top-notch security assurance on mobile devices. While current smartphones or tablets already have strong security in place to fend off possible tampering, the security-dedicated chip adds extra countermeasures to defend against possible attacks such as reverse engineering, power glitches and laser attacks, making it extremely harder for others to access or copy stored confidential data.

In addition, the SE solution manages failed attempts and prevents replay attacks by accepting only the latest authentication request as a valid one Samsung's new SE solution is currently in mass production and is featured in Samsung's recently-announced Galaxy S20 series smartphones.

# KEEPING CITIES SAFE IN THE AGE OF SMART TECHNOLOGY

By CJ Chia

More than half of the world's population currently lives in cities, a number that will continue to rise as the number of cities increase and more countries become more urbanised. With this trend, making sure our cities are safe is increasingly important, yet it is also one of the biggest challenges of urbanisation.

There are various ways in which to measure safety, with one of the most comprehensive measurements being provided by the Safe Cities Index (SCI). This benchmarking tool by the Economist Intelligence Unit, sponsored by NEC, measures a wide range of security inputs and results and assesses the relevant strengths and weaknesses of over 60 major urban areas worldwide.

Urban safety is by nature multifaceted; it goes beyond simply looking at cybersecurity or physical safety. Reflecting this, the SCI uses indicators which are divided into four distinct pillars: digital, infrastructure, health, and personal security. The index is also regularly updated, with the 2019 edition adding a focus on the concept of resilience: the ability for urban areas to bounce back after a natural or man-made shock.

To measure safety, SCI examines indicators which are grouped into inputs of safety; policies or personnel dedicated to an aspect of security, as well as outputs; outcomes like air pollution levels and crime rates which show how safe a city currently is. For example, to measure Digital Security, elements like the city's digital privacy policy and citizen's awareness of digital threats are taken into account, measured alongside outcomes like the percentage of computers infected and the risk of local malware threats.

*Keeping cities safe is key to raising quality of life and keeping the place running smoothly. It is, however, a massive challenge that has evolved in the face of technological advancements.*

Despite tracking performance across four pillars, findings show that performance in any single area tends to correlate with the city's performance in other pillars. For example, investment in cyber-protection is important for multiple aspects of security. Likewise, a glaring weakness in any one area tends to undermine multiple areas of security.

## The Framework For A Safe City

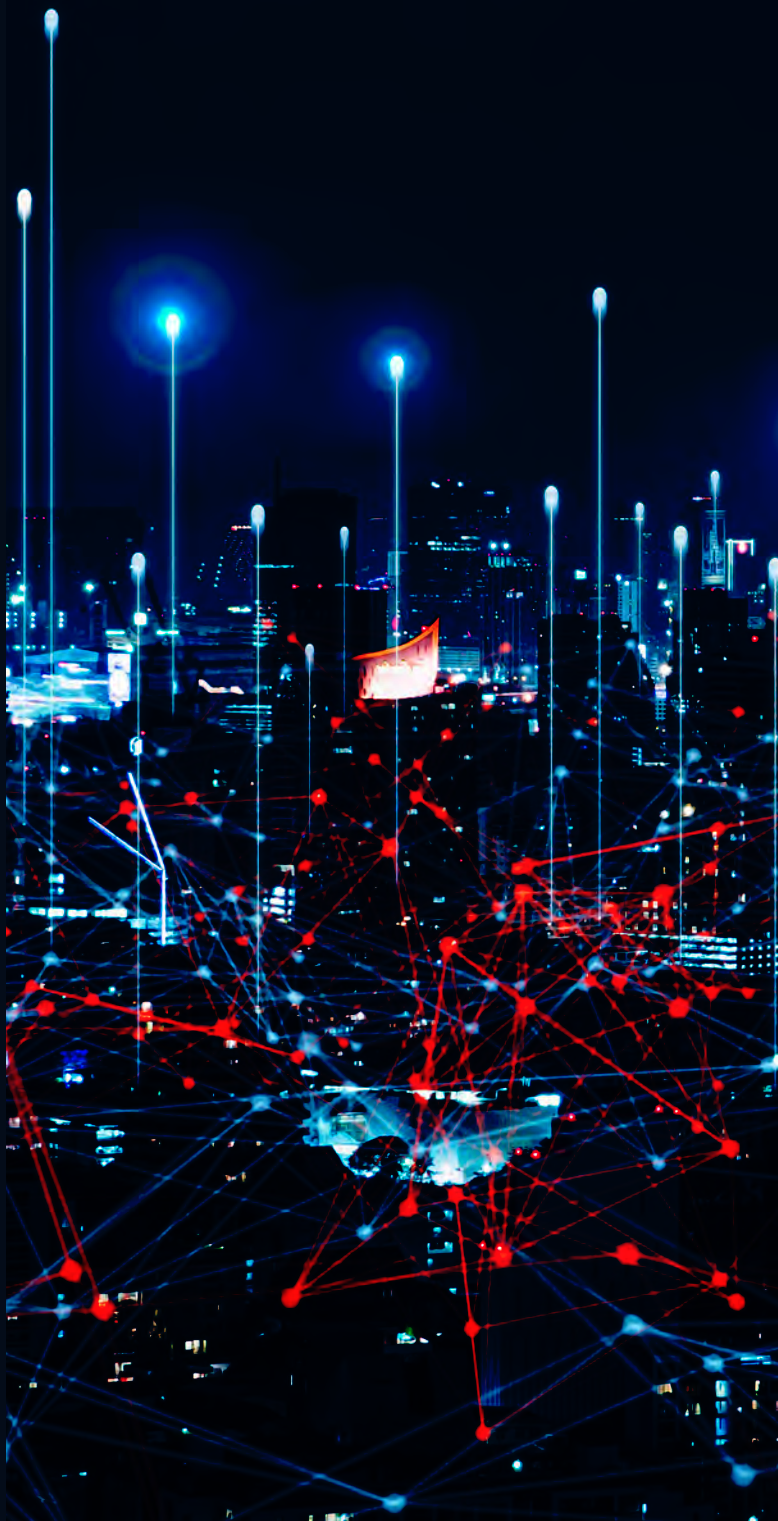
Safe cities provide the necessary security and safety that is needed to keep citizens safe from all manners of threats like crime and terrorism, while also mitigating the impact of natural disasters and any threats that might occur. To be effective, a city's safety framework needs to take into consideration the support that relevant agencies need before, during, and after an event.

The first aspect of a good safety framework is prevention. Security measures need to be put in place that predict threats and hazardous situations, and authorities should be able to use this information to prevent threats from even occurring in the first place. Simulation and forecasting technology based on big data mining can be key here; by predicting crowd turnout for an event, for example, organisers can more effectively allocate security resources as a deterrence.

But even the best laid plans fail. While preventive measures help to reduce the occurrence of hazardous situations, unforeseen events can still occur. This makes detection and response key parts of a city's safety framework.

Measures concerned with detection tend to revolve around helping public-safety organisations to collect, share, and analyse data to more effectively provide early warnings, and help increase awareness on the situation as it unfolds. This can be achieved through the use of sensor systems that range from video surveillance cameras, weather sensors, and even CBRNE (chemical, biological, radiological, and nuclear) sensors. Some, like weather sensors, can help to detect inclement conditions early, giving authorities time to evacuate necessary areas, while others, like gunshot sensors, can provide real-time alerts as events occur.

In order to make detection effective, response is another key aspect of a city's safety framework. There is a need for measures that enable key organisations to react to security threats quickly and effectively in order to minimise the negative impact of a security threat, and to prevent adverse events from escalating. Besides having comprehensive response plans in place, tools like consolidated ICT platforms can be of great help by providing a common operational picture to relevant agencies, raising the situational awareness across different response teams, and allowing for better coordination in their responses. When discussing safe cities, we should not forget another important stage in the safety framework: recovery. During



and after a security incident, it's important to rescue victims as soon as possible, as well as to examine and analyse the factors or lapses that allowed the incident to happen, and what can be done to prevent or minimise the impact in the event of future reoccurrence.

## Safety Through Technology

With technological advances, it's hardly any surprise that smart technology and devices are instrumental in increasing safety in cities these days. With highly accurate sensors and integration with machine learning, it is now possible to monitor a city and its citizens on a scale that would have been absolutely unviable several years ago. Where previously security had to be increased by adding more personnel, one can now employ surveillance tools to be your eyes on the ground, leaving organisations the flexibility of reassigning manpower more effectively.

As such, it can be said that safe cities are inextricably linked to smart cities. While technology cannot cover aspects of safety like policy making, it has shaped the way that governments and organisations plan to make their cities safer. However, it is important to note that technology does not have to be smart to make a city safer.
There are many examples of technology that directly contribute to making cities safer, including:

- **Artificial Intelligence (AI) Integration**

By adding AI integration to existing security solutions, it becomes possible to take their usefulness to a new level. Instead of needing a human to look through surveillance footage for it to be useful, AI allows for the analysis of life footage without human intervention. Footage from a video camera can be checked against a facial recognition database, and trigger alerts should high security risk targets be spotted.

Other applications include AI that recognise gunshots or aggressive behaviour, and trigger an alarm when these occur, allowing authorities to respond quickly, and also allowing them to be better prepared for the situation on the ground as it unfolds.

- **Body-worn Cameras**

Body worn cameras can provide an additional perspective that stationary cameras cannot offer and helps to keep both citizens and the security personnel that are using it safer. With knowledge that their actions are recorded, police officers and security officers will hopefully be discouraged from acting against protocol, while potential troublemakers might be deterred from acting out, knowing that there is a high likelihood they will be identified otherwise.

- **Smart Street Lighting**

Street lights that are connected to a network can do more than provide lighting. Embedded sensors can also be used to monitor air quality, humidity, and temperature amongst

other things, allowing governments to better manage traffic networks and keep track of environmental health and safety.

• **Security Drones**
Technology like drones provide alternatives with a significantly lower skill ceiling for security personnel to utilise when necessary. An aerial perspective can be invaluable when a security incident takes place in a high-rise building, and drones offer this advantage for a lower cost than helicopters, while also having the potential to perform well even in poor weather. The unmanned nature of these drones also keep security personnel safer while performing reconnaissance. These drones can also cover more ground than a person might be able to, and thus has higher potential to do a sweep of an area during surveillance.

Technology contributes more to safe cities than increasing surveillance and improving monitoring. More advanced urban planning tools also mean that safe cities have more accurate and detailed information to work with. An urban planner who has a better view of pedestrian behaviour and traffic trends in an area is better able to plan for safer roads—perhaps an area with high incidences of jaywalking could do with more crosswalks.

## Paying For Security Through Privacy

One concern when it comes to creating safer cities through technology is the possible loss of privacy. With increased surveillance, citizens might feel that their privacies are at stake—no one wants information like when they went to the supermarket to be easily available unless it is necessary.


This is unquestionably a challenge. When using an app, the user is able to check a dialog box that consents to how their personal information is used, with some more robust privacy options allowing the user to control what is shared and what is not. This becomes difficult in public spaces; there's no simple way for people to opt out of giving their consent of being recorded in a crowd.

It might seem simple to just not attach personal information to data in order to address privacy concerns, but doing so cripples the good that these systems bring to making cities safer in the first place. Instead, cities should consider putting in place robust privacy laws and rigorous data encryption to assuage the privacy concerns of the population without compromising on the usefulness of data collected.

• **Encryption Of Personal Information**
Proper encryption of personal information means that analysts can link together personal data, but that results are anonymised and aggregated. This will prevent data scientists from identifying specific behaviour patterns of individuals, instead allowing it to be read as something like "Person A of age group 41-50 in the town of Wellington spends 26% of their time on public transport, similar to 30% of those in this demographic."

• **Audit Trails**
In order to prevent misuse of data, it's important that a data solution has in place audit trails that identify key details like when certain data was accessed, by whom, and for how long. This makes it easier to inspect how data has been used, and penalise misuse as necessary. An example of this would be customer data for a single organisation—it's often necessary for customer officers to access this information in order to assist the customer, but there have been multiple cases of misappropriation of this data. Proper audit trails have helped to identify the culprits in these cases. This is even more important if the government outsources the analysis of its data to a vendor.

• **Transparency Of Privacy Policies**
To address privacy concerns, it is also imperative that organisations are transparent about policies like how long the data is kept in the database, what this data is used for, who has access to it, and whether or not this data is disposed of in secure ways. It's also important to be transparent should data breaches occur—hushing up these incidents only serves to make people question the situation more. One needs look no further than the recent Travelex cyberattacks to see how silence can create massive loss of public confidence.

• **Clarity On How Data Is Kept Secure**
While it certainly is impractical and deadly to reveal your cybersecurity measures, there is a necessity in giving enough information to assure the public that their data is kept safe from cyberattacks, rather than being kept in unsecured ways.

## The Importance Of Safe Cities

Cities that are recognised as safe tend to have stronger and more stable economies. Take the city of Hong Kong as an example. The unstable climate created by the protests have led to uncertainty in investors, some of whom have reacted by pulling investments out from the city and diverting them to other cities like Singapore.

Citizens who enjoy peace of mind that their safety is assured also raises their quality of life, which in turn means they are more productive.

At the end of the day, the growth and success of a city can be said to be reliant on how safe it is deemed to be by citizens, and foreign investors. This makes it a key area of concern that should not be overlooked by governments, even in the face of changing challenges presented by the digital age.

# How Can A Digital Twin Create A Seamless Workplace For Employees?

*Digital twins solve the challenges of real-time data processing by bringing together data from IT and OT systems, IoT sensors and third-party data in a contextual representation of your built environment.*

**By ThoughtWire, published on IoT for All**

How can a digital twin create a seamless workplace for employees? Before we answer that question, let's first define what we mean by a digital twin. Not simply a digital mock-up of the physical environment, a digital twin is the contextual model of an entire organisation and its operation. It's the data from your subsystems and the real-time interaction between your people, process and connected things.

Digital twins solve the challenges of real-time data processing by bringing together data from IT and OT systems, IoT sensors and third-party data in a contextual representation of your built environment. They allow you to analyse the complexity of your built environment across the entire portfolio, take immediate action to optimise conditions, and track and improve the state of your built environment over time.

### Digital Twins Help Create Dynamic Spaces

The way we work is changing. If you look at industry news headlines, you'll see articles about the rise of shared working spaces, flexible work hours and remote working. Yes, Millennials and Gen Z'ers are big drivers of this change, but the conversation isn't limited to the younger generations.

In fact, in today's economy, there is a multigenerational global talent war in many industries — like tech, finance and telecom — where workers of all ages and demographics are asking for flexible working arrangements, remote work and a more holistic perspective on productivity in exchange for their loyalty. Moreover, in our increasingly connected world, employees want their office environments to be as smart as their homes, cars and digital communities, with the ability to create a personalised experience.

However, many traditional office buildings still operate in the "dark" with limited use of modern technology and little ability for employees to interact dynamically with their environment. Not only does this make for an experience marked

Designed by Freepik

by friction, it leads to inefficiencies in building performance and to missing out on the "wow" factor — something that helps attract in-demand employees.

A digital twin can transform an outdated workplace into one that's dynamic, modern and seamless. By bringing together information and data from a variety of different sources and producing a contextual model, a digital twin can be used to optimise conditions and enable employees to interact with their spaces. For instance, if a group of employees needs to work collaboratively on a certain project, digital twin technology can be leveraged to match the group with a space in the building that offers the right features; they can book it and enjoy control over the conditions of the room.

### Digital Twins Provide Missing Insights About Building Usage

Do you truly know how employees are using your building? For instance, are there empty boardrooms with lights left on for hours at a time? Are there times when an entire floor of employees leaves for a team retreat or conference? Are there certain days of the year when specific teams or companies are working round-the-clock to meet deadlines?

How people interact with their office environment directly impacts resource use and needs for services like cleaning and security. By having better insight into how and when people use a space, you can find ways to scale resources up or down or enable a more flexible use of the space. A digital twin uncovers these missing insights by providing 360 dashboards, floor plans, analytics and other tools that offer information about real-time building use. A digital twin also helps to predict future states and to optimise conditions, resulting in better outcomes for everyone, including reduced costs for owners and a seamless experience for employees.

### Digital Twins Supply Data to Make Business Decisions

Now, more than ever, building owners and operators are looking to data to make business decisions. Data is all around us, yet harnessing data in a way that allows us to operationalise it has been a challenge. Digital twins change this. By providing a holistic view of a building, they unlock data that was previously hidden and test how this data can result in positive outcomes for both the bottom line and employees.

With access to actionable data, digital twins can help owners / operators make better decisions about a range of topics and economic drivers. For instance, third-party service contracts can be better negotiated and deployed when informed by data from a digital twin. Rather than use a static model for making decisions on services like cleaning or maintenance, owners/operators can employ a demand-based model that matches supply with changing needs. This makes for a smarter approach, resulting in better working conditions for employees and reduced costs for building owners.

**In conclusion, digital twins are transforming the built environment and creating seamless employee experiences. With digital twin implementation on the rise, new use cases are being developed every day, and the technology is helping owners future-proof their assets and attract in-demand employees by offering a superior experience.**

### Digital Twins Improve Employee Experience

How many times have you been too hot or too cold in your office building? How many times have you visited the washroom and found no hand towels? How many times have you reported a light out and waited days or even weeks before it was changed? Communication in a large office building is difficult. With literally hundreds of occupants, dozens of bathrooms and thousands of lights, building managers get endless requests and struggle to triage and action them all in an efficient manner. This is just one contributing factor that can make for a clunky employee experience.

A digital twin changes this by bringing together data from connected devices and sensors to provide building managers with real-time information about changing conditions. Is a light out? An IoT sensor will alert the building manager. Is an employee feeling too cold? Using their connected smart phone app, the employee can change their environmental settings. Digital twins also help determine the most efficient path to action requests and allow dynamic two-way communication between building staff and employees.

In conclusion, digital twins are transforming the built environment and creating seamless employee experiences. With digital twin implementation on the rise, new use cases are being developed every day, and the technology is helping owners future-proof their assets and attract in-demand employees by offering a superior experience.

# How Businesses Need To Show How AI Decides

*As artificial intelligence becomes more widespread, the need to render it explainable increases. How can companies navigate the technical and ethical challenges?*

**By Lindsay Clark, ComputerWeekly.com**

Show your working: generations of mathematics students have grown up with this mantra. Getting the right answer is not enough. To get top marks, students must demonstrate how they got there. Now, machines need to do the same.

As artificial intelligence (AI) is used to make decisions affecting employment, finance or justice, as opposed to which film a consumer might want to watch next, the public will insist it explains its working.

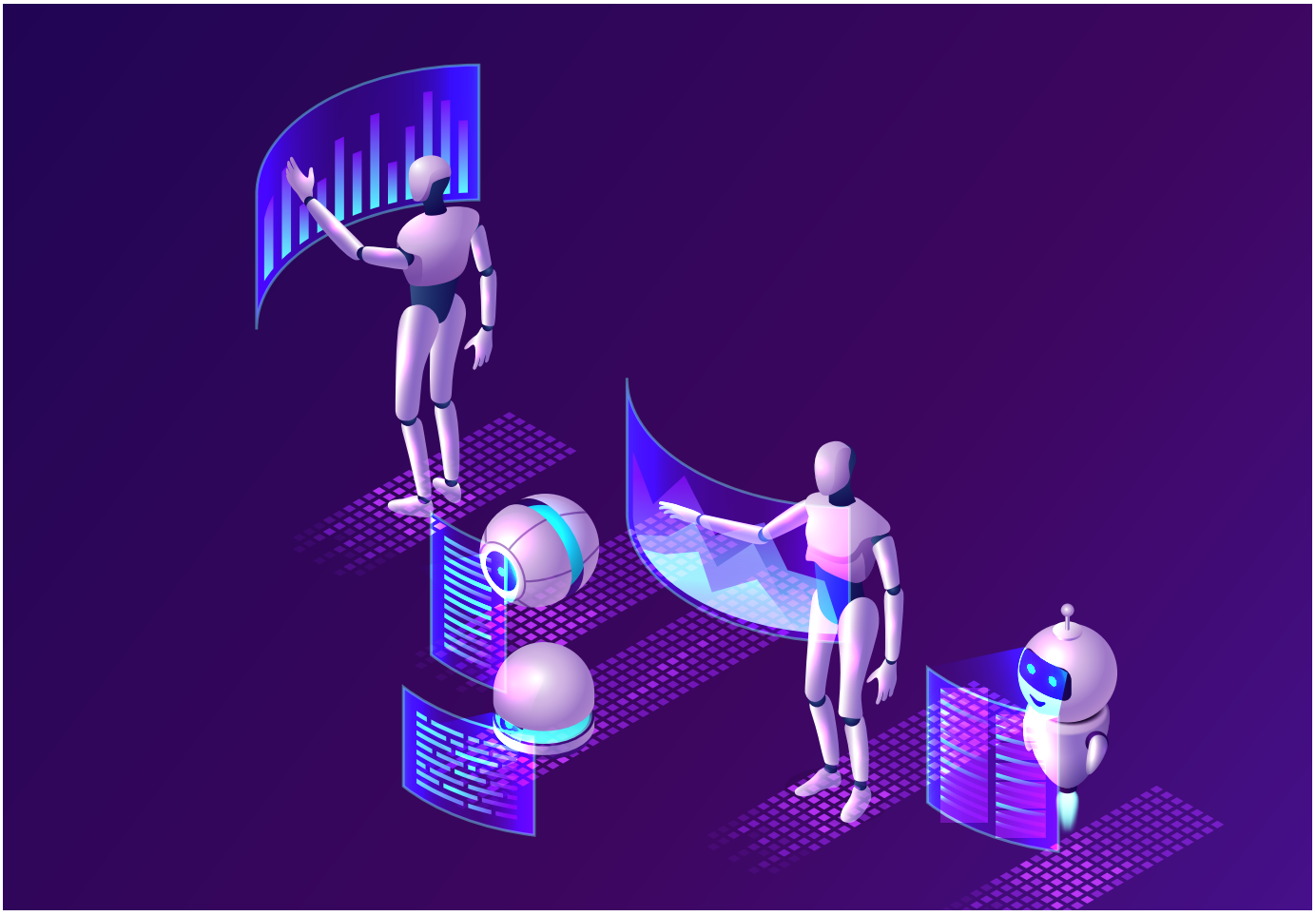
Sheffield University professor of AI and robotics Noel Sharkey drove home the point when he told The Guardian that decisions based on machine learning could not be trusted because they were so "infected with biases".

Sharkey called for an end to the application of machine learning to life-changing decisions until they could be proven safe in the same way that drugs are introduced into healthcare.

And the IT industry is waking up to the threat to the next big wave of spending.

Although he does not use the same language as Sharkey, Patrick Hall, senior director for data science

Designed by vectorpouch / Freepik



Designed by upklyak / Freepik

products at machine learning tools company H2O.ai, says decisions that cannot be explained will feel very "icky" to consumers.

"Companies are starting to be aware that they need to create explainable AI to satisfy human curiosity," he says. "We are trying to get business adoption of this cool, new, very powerful technology and are trying to prevent this icky 'computer says no' feeling."

In a study based on interviews with 4,400 consumers, Capgemini found that their views on ethics and AI threaten both company reputation and the bottom line – 41% said they would complain in case an AI interaction resulted in ethical issues, 36% would demand an explanation, and 34% would stop interacting with the company.

The results show that although machine learning ethics and explainability are separate issues, they are linked, says Hall. "The way to test for bias in data and machine learning models is a fairly well-known process called disparate impact analysis, which is different, technically, from explainable AI," he says. "They certainly do go together, but I would never use explainable AI as my front-line, fairness testing tool."

**In a study based on interviews with 4,400 consumers, Capgemini found that their views on ethics and AI threaten both company reputation and the bottom line – 41% said they would complain in case an AI interaction resulted in ethical issues, 36% would demand an explanation, and 34% would stop interacting with the company.**

### Tools To Explain AI

To help organisations explain their machine learning decision-making, H2O.ai has created a set of tools that provides companies with dashboards to explain the results

of both their own driverless AI models and models built through other processes. These include:

- **LIME (local interpretable model-agnostic explanations)**
  The technique attempts to understand the model by altering the input of data samples and understanding how the predictions change.
- **Shapley values**
  Using game theory to assign importance to machine learning features indicating which is likely to lead to a decision.
- **Partial dependence**
  The marginal impact of a feature on model prediction, holding other features in the model constant.

In August 2019, IBM launched a set of tools designed for a similar purpose. AI Explainability 360, the company says, is a "comprehensive open source toolkit of state-of-the-art algorithms that support the interpretability and explainability of machine learning models". IBM is inviting the open source community to contribute to expanding it.

Saska Mojsilovic, an IBM fellow focused on AI, says businesses will have to adopt explainable AI because they need to get consumers to trust the machine learning model they are adopting with increasing frequency.

"It became very obvious that if you are going to be using these machine learning algorithms to inform, or guide some really important decisions in our lives, then you really need to have this confidence or trust," she says.

But explaining machine learning decision-making to a data scientist is one thing; explaining it to consumers or the public will require a great deal more creative thinking, says Mojsilovic.

"Fairness may be a complex ethical issue, but in a way, explainability is even more difficult," she says. "Think about how humans explain things, how we navigate the world around us and how we communicate. We do it in so many different ways. We look for examples and counterexamples and summarise things, and so on. We thought about how to take that expressiveness of human interaction and create the methods to communicate [the way AI reaches conclusions].

"There are these ways to get to an explanation. So, over the last year or a year and a half, we created several models that employ these different modes of human explanation."

For example, IBM has created a model called ProtoDash that explains the results of AI using prototypes – examples of the kinds of scenario that drive predictions. Meanwhile, a model called Boolean decision rules generates sets of rules that humans find they can interpret, a method that won the inaugural FICO Explainable Machine Learning Challenge. Lastly, there is an approach that relies on the concept of "contrasting explanation" which tries to pick out things that are missing.

"Doctors, for example, tend to diagnose patients as much on symptoms that are not present as ones that are," says

*Designed by Freepik*

**"Organisations need to think about their particular use case and not see AI as a kind of magical entity that is making everything better," she says. "Yes, we've made concrete advances in certain areas, but there are other areas where we have not at all. The whole idea of the premise of trying to predict what a person is going to do in the future is very dubious."**

Mojsilovic. "If something is missing, it is an important differentiator. Had it been there, the decision would have been vastly different."

### The Governance Imperative

But the challenge of creating AI decision-making that companies can explain is not only about the tools and technology, says Sofia Ihsan, trusted AI lead at global consultancy EY.

"When I'm doing some of my work, I'm often in a room for PhDs – some really clever data scientists," she says. "If you look at what motivates them, it's about accuracy – explainability isn't something they are thinking about. At least, it's not their primary consideration. When they do think about it, they might think it is a limiting factor and they don't want to be limited."

So, creating an overall governance structure that includes explainability in the AI process from the outset is a struggle for many organisations, says Ihsan. "When you think about training data, that's right at the beginning of the lifecycle of development."

Explainability needs to start at the beginning, she says. "It's not about coming in after the event and trying to put controls and assurance in place. It is about identifying and managing risk throughout the lifecycle of development and monitoring them while models are in use to make sure that they are working in the way you expect them to work."

Such is the growing public interest in the fairness of AI decision-making, building in explainability from the start will come under the umbrella of corporate social responsibility, says Ihsan.

"What is the impact on society, on mental or physical wellbeing, and the environment?" she says. "The public is generally getting more savvy. This is going to come in from a brand perspective. People not only want to know that they're being treated fairly as individuals, but also more broadly, that things are fair and unbiased."

But for AI to be accepted on ethical grounds, it will require more than simply explaining the reason behind machine learning decisions, says Rachel Thomas, director of the University of San Francisco's Center for Applied Data Ethics.

"When AI makes decisions that really impact people's lives, then not having an explanation is incredibly frustrating," she says. "But an explanation alone is not sufficient. There needs to be some sort of system for recourse as well, such as the ability to appeal decisions."

The difficulty of building explainable AI from the start, and offering a justification for decision-making when challenged, is tempting some organisations to skip some of these processes, says Thomas.

"It's called 'fair-washing', where people take an unfair system and post-hoc give a fairer justification for the decisions they have made," she says. "If somebody misses out on a loan because of their gender, and then you could go back later and say, 'oh no, this is because of their credit score'. You can always find an explanation that is less suspect. It is another reason why explainability, in itself, won't be sufficient [to create ethical AI]."

Some organisation have promised AI that helps with hiring decisions or predicting crime, but Thomas warns businesses against the blanket adoption of AI in all use cases.

"Organisations need to think about their particular use case and not see AI as a kind of magical entity that is making everything better," she says. "Yes, we've made concrete advances in certain areas, but there are other areas where we have not at all. The whole idea of the premise of trying to predict what a person is going to do in the future is very dubious."

As the popularity of AI spreads, so does public concern about its impact. Only AIs that can explain their decisions in a way people can understand and accept will create long-term value for the organisations that create them.

# Small Business Cybersecurity Threats And How To Fix The Fox

*Your business might not be on the Fortune 500 list, but that doesn't guarantee that it's threat-free. If you think hackers attack only the big boys and girls, you may be shocked by these stories. Here are small business cybersecurity threats and how to fix the fox.*

**By Ejiofor Francis, Founder of EffectiveMarketingIdeas**

Do you know that Escrow of California was forced to shut down when cyber-thefts nabbed $1.5 million from its account? These criminals gained access to the company's bank data using a form of "Trojan Horse" malware.

Green Ford Sales, a car dealership in Kansas, lost about $23,000 when hackers broke into their network and swiped bank account information.

Many cybersecurity issues go unreported and rarely make news headlines.

One shocking incident was when cyber-thieves drained $1 million from the bank account of real estate development firm Wright Hotel. They gained access to the company's email and used the gathered information to impersonate the owner. These hacks convinced the bookkeeper to wire money to an account in China.

Designed by Freepik

Symantec, one of the leading cybersecurity companies in the world, also affirmed in a report that attackers target both large and small businesses.

There are several common cybersecurity issues which your business should be wary of, as well as some practical ways in which you can fix the fox.

### #1 Watch Out For Ransomware Attacks

Ransomware is one of the most common methods hackers implement and many small businesses have been ruined because of it. Simply defined, ransomware is malicious software that takes over your company's system and demands that you pay a ransom to cybercriminals to get back your stolen data.

Designed by macrovector / Freepik

According to research by Cyber Security Ventures, a new ransomware attack occurs every 14 seconds. The total number of ransomware attacks will hit 11.5 billion by 2020.

Sadly, a ransomware attack can put you out of business because the cost to recover whatever the hackers stole from your company can be outrageously high.

Practical measures that can save your business from getting attacked by ransomware include:

- Always keep your operating system (OS) patched and up to date: If you're clueless on how to handle this, you might want to hire an IT expert to oversee this. Also, make sure each of your employees adhere to this rule in order to prevent loopholes through which an attack can be made.
- Install antivirus software that can detect malicious programs like ransomware as it attempts to feast on your network, and also use a whitelisting program that restricts unauthorised applications from being executed.
- Do not install any program or software unless you're fully aware of what it is and how it works.
- If your business can hire an IT expert, make sure that you hire someone ready to take your business safety seriously as if it was their own. If you can't hire an expert at the moment, at least ensure that you and your employees do the necessary to keep your systems safe.

### #2 Watch Out For Spear-phishing Attacks

Phishing is another serious cybersecurity threat that's trending. This malware tends to target organisations through your email inbox.

Individuals and organisations alike are often eager to find out what's in the box, and this form of attack exploits that eagerness. It appears as a friendly, unassuming email, instant message, or text message that you might not be suspicious of and be tricked into opening.

Trend Micro, a security software firm, reported that 94% of targeted emails use malicious file attachments as the infection source. The firm also revealed that 91% of cyber-attacks begin with a "spear-phishing" email.

Research also estimated that there are around 400 phishing attacks every 24 hours and nearly 30% of them are successful.

There are a lot of phishing email formats that hackers use to cajole people into clicking an attached link within the email, and the first line of prevention is to be very cautious with any messages you open.

You may also wish to arrange seminars and training workshops on cybersecurity awareness to keep you and your employees updated on the latest developments, as well as best practices to follow.

There are a lot of benefits associated with this. The training will keep you and your team informed on the increasingly sophisticated attacks that you might come across, and will also teach you and your employees how to identify phishing emails that you come across them.

### #3 Watch Out For BYOD (Bring Your Own Device)

BYOD can be a great policy. It's convenient and efficient for employees who might need to work while mobile. At the same time, you shouldn't neglect the risks that come with this practice. Small businesses are very much vulnerable to data theft, but the risks increase when employees are using unsecured mobile devices to share and access sensitive data.

To prevent your company from being a victim, you should establish a rock-solid BYOD policy that every employee will understand and adhere to. This policy should aim to educate your employees, and ensure that their devices will only have access to the company's network through a secured channel.

In addition, you'll want to ensure that all connected devices have proper antivirus and firewall applications installed.

### #4 Watch Out For Fraudulent Apps

Did you know that not all the apps you find in the app store are completely safe to download and install? Hackers have leveraged this opportunity by creating some work-tool apps that boost daily productivity, but come with an added gift of malicious code.


Once an employee that handles sensitive information installs the app, the code might give hackers access to the company's personal data. Hackers can also use these malicious apps to breach the company's network once the employee's device is connected.

Some ways in which this can be fixed include:

- Keep all personnel in your company aware of this type of threat. Have visible warnings reminding your employees not to download apps just because the reviews might seem appealing.
- Set up a process where employees will need the approval of your company's IT team before installing any third-party apps.
- Make sure your services are up to date. Outdated services put your business at risk.
- Consider up-skilling members of your company's IT team.

### #5 Watch Out For Weak Passwords

Weak passwords have allowed cybercriminals to wreak havoc on many small businesses. If you and your


Designed by Freepik

employees are still ignorant of this fact, then your company might be vulnerable to this threat.

- A study on "The State of Cybersecurity in Small and Medium-size Business" was carried out by the Ponemon Institute in 2018. They reported that 60% of those surveyed revealed that negligent employees were the root cause for data breaches, as compared to 37% that were attributed to external hackers.
- About 32% of respondents said that they were not able to state the cause of their data breach in the last 12 months. Additionally, about 40% of respondents said that their companies experienced data breaches due to compromised passwords in the past 12 months.
- Around 19% of IT and security professionals believe that password protection and management will be increasingly critical to data and network security.

A better way to improve your company's encryption and authentication process would be to:

- Implement a two-way authentication method instead of a regular password that is more easily hacked.
- Implement a biometric authentication method.
- Implement training that will educate you and your employees on how best to manage and secure passwords.

### #6 Watch Out For DDoS (Distributed Denial of Service) Attacks

Small businesses still regard DDoS attacks as an old internet threat when they are in fact a very much real and current threat. Did you know that DDoS attacks doubled in 2017, and the number of attacks is still growing?

If you've been overlooking the effect of this form of attack, I'd advise you to relook your security processes. This attack

**A DDoS attack will direct a huge amount of web traffic at your website, slowing down your website's speed considerably, and can even take down the entire server where your website is hosted. DDoS attacks can make it difficult for customers to do business with you through your website. Consequently, you might end up losing both your customers and revenue.**


is not only capable of compromising sensitive data, but can also damage the quality of services you offer. A DDoS attack will direct a huge amount of web traffic at your website, slowing down your website's speed considerably, and can even take down the entire server where your website is hosted. DDoS attacks can make it difficult for customers to do business with you through your website. Consequently, you might end up losing both your customers and revenue.

It's impossible to completely prevent a website from being targeted by DDoS attacks, but you can strategically minimise the effects using the following methods:

- Make sure that there is extra bandwidth available for your website. This will give your server more room to accommodate unexpected spikes in traffic.
- Revamp the security of IoT devices that you and your employees are using.
- Monitor your website's traffic levels constantly.
- Hold workshops that will train your staff on how to handle DDoS attacks, and implement procedures which they can follow in the event of an attack.

Your best defence might be to go on the offense. Attacks might still target you, but you can minimise the impact by working directly on a fix for each cybersecurity issue.

Your business will be less likely to fall victim to cyberattacks if you and your employees all stay alert to the dangers of attacks and take the necessary precautions.

Designed by rawpixel.com / Freepik

# Working Smarter: The Intelligent Office

*IoT is not only changing the way we live, but it's also changing the way we work. Connected devices are enhancing the employee experience and impacting the way offices are designed, to stimulate optimal productivity and creativity.*

**By Anoop Nair, Senior Director of Software Technology and Architecture at Flex**

Smart houses, smart cars, and smart cities – each of these environments benefits from the 8.4 billion connected devices expected to fill the world this year. The Internet of Things (IoT) is an evolving ecosystem of smart living and connected devices that work together to create better capabilities, efficiencies and most importantly, experiences. It also affects our time in the office, where Gallup says we spend up to 47 hours per week. IoT devices are changing the way we think about office design, the employee experience and creating environments for optimum productivity and creativity. Smart technology is enabling more intelligent offices.

Intelligent products and services control lighting and temperature, help us find quiet spaces to think and highlight ways to connect effectively with our colleagues. Here's a closer look at trends in intelligent products and services we're watching at Flex, which fuse form and function in ways that optimise people's experience in the office, enabling them to be their best, most productive selves at work.

Designed by macrovector / Freepik

### Smart Lighting

IoT lighting devices help create office environments that use lighting to optimise productivity and even creativity. Guided by smart software, systems may allow users to dim and brighten lights via a smartphone app. Today's more sophisticated systems use sensors in lighting fixtures to brighten and dim in response to natural light levels, continuously optimising the environment throughout the day. Circadian systems use sensors to sync lighting with the time of day, offering bright, cool light to help teams launch into action in the morning and gradually softening throughout the day. It's even possible to use smart lighting to create diffused light, which promotes creativity. A report by BI Intelligence shows IoT lighting can help cut costs. In one example, the use of smart LED lighting reduced energy costs by 75% while productivity increased by 20%.

### Ambient Temperature Control

Smart technologies are automating ambient temperature. An IoT-powered desk by Arup uses sensors that give individuals control over the temperature in their immediate environment, which is especially relevant in today's largely

open-floor-plan offices. Systems can track heat signatures throughout a building to determine whether they're too warm or too cool, and based on occupancy detection and measures of air quality, they can adjust the HVAC settings. Not only does this enable more control for individual employees, but it helps us more proactively manage energy costs and contributes to sustainability initiatives.

### Live Mapping

Live mapping technologies use a mix of beacons and sensors to help users more effectively navigate their offices. Need to know which conference room is available, whether a bathroom is in use, or which space is most likely to yield the quiet time needed to solve a complex problem? A number of different technologies help us better understand how spaces are used and occupied. The data helps commercial real estate professionals optimise the tenant experience and helps the average worker seamlessly move through their day while cutting out unnecessary steps.

Enlightened, for example, put sensors into fleets of LED lights and uses software to track movement against a building plan. Users can gather data on energy usage, control HVAC and more. IoT technologies are even helping us better manage collaboration and face-to-face time. Humanyze's badge module tracks in-person meetings, management visibility and the tones of voices and movements (via infrared) that lead to successful business outcomes.

### Ergonomics And Wellness

The U.S. Occupational Safety and Health Administration (OSHA) estimates that employers pay almost $1 billion per week treating the effects of poor ergonomics. IoT devices are changing the way businesses design office environments to support employee health and wellness. The Stir Kinetic desk is a hybrid standing and sitting desk controlled via a touch screen and using cloud-based architecture to store individual profiles and preferences. Sensors monitor how much users sit and stand daily, sharing that information with them, as well as providing "WhisperBreath" reminders via a slight shift in desk position when it's time to move. Smart chairs are being constructed with sensors to alert employees when their posture is bad and provide recommendations for improvement.

### Integrated Workplace Platforms

The full promise of the smart office comes into focus when a single hub is used to pull together insights from different platforms. Research and Markets predicts that the IoT integration market will reach $22 billion per year by 2022. With integrated workplace platforms, organisations and individuals can do the following:

- Get a full picture of an individual worker's day, from biometrics and stress levels to productivity and locations throughout the office, to provide actionable insights and coaching to improve performance.
- Employ automated systems that streamline and optimise the ambiance of any office, for maximum comfort, productivity or other goals.
- Utilise smart, data-driven platforms that help organisations understand all aspects of physical office space use and guide decisions from cost-saving strategies to informed architecture and design strategies.

While the impact of IoT has begun to mature and achieve significant results in areas such as manufacturing and industrial operations, we're at the beginning of the curve for smart products in the office. Innovative IoT tools are helping employees and businesses make better decisions about day-to-day activities and long-term operations. For product creators, this is a market with significant opportunities, where start-ups and enterprise players have only begun to scratch the surface of what is possible.

Designed by macrovector / Freepik

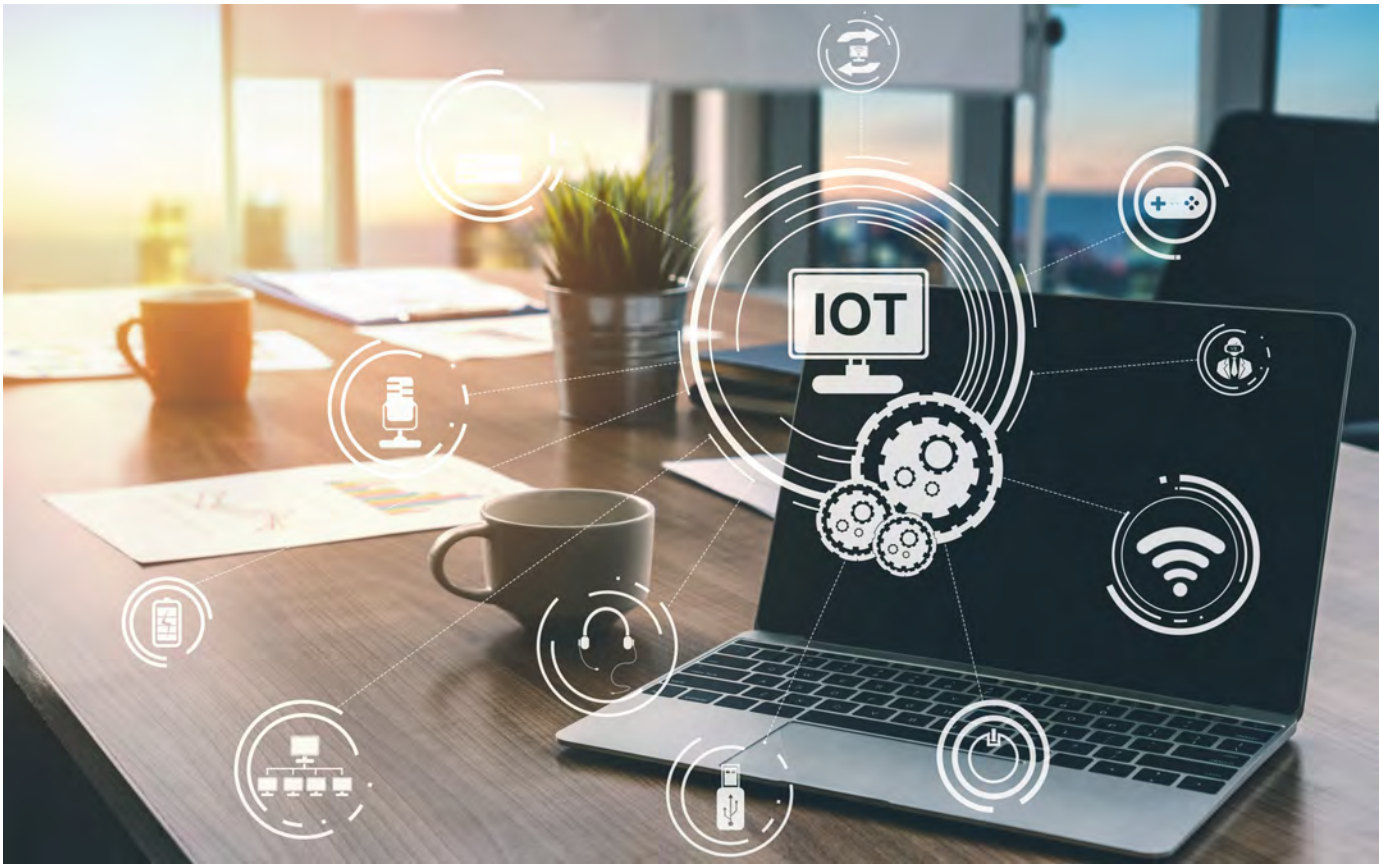
# Increasing Business ROI With IoT In Facilities Management

*Thanks to the advanced technologies, the idea of smart offices is now becoming more trendier than ever. It's just a matter of time until the majority of businesses will have intelligent offices. As the workplaces are getting smarter, the one thing that remains obsolete is the way facility management companies operate.*

**By Michael Georgiou, Co-founder and CMO at Imaginovation**

Keeping various supplies in check is a tedious job for busy offices. That's why often such non-core tasks are outsourced to facilities management companies. Today's tech-heavy environment, offices still have to make calls or send emails to their facilities manager to get the issues resolved.

Considering the fierce competition, FM business owners can't simply afford to keep offices waiting. Enter the IoT (Internet of things). IoT is a network of physical devices that collect and share data over the Internet. Using IoT, facilities management companies can drastically improve their efficiency, customer relationship, and business ROI. But,



**IoT is a network of devices or "things" connected to the internet. The objects in IoT are loaded with sensors that collect and share data with different other devices in the network. IoT essentially enables different machines and objects to communicate with each other.**

how exactly IoT benefits facilities managers to improve their business bottom line? In this guide, we're going to discuss this in detail, but let's first understand the concept of IoT.

### What Is IoT (Internet of Things)?

IoT is a network of devices or "things" connected to the internet. The objects in IoT are loaded with sensors that collect and share data with different other devices in the network. IoT essentially enables different machines and objects to communicate with each other.

A simple example of IoT in action is the smartwatch. Your smartwatch tracks your physical activity, such as the distance you run and then sends this data to the app or email. Modern applications of IoT are much more advanced than this, especially in the case of smart or intelligent offices.

According to the Intel report, the number of IoT devices will reach 200 billion by 2020. A report published on Gartner predicts that more than 65% of all the business organisations will have IoT products by the end of 2020. With IoT technology, FM companies can implement low-cost sensor devices to get contextualised data in real-time and make informed decisions on time.

### How IoT Benefits Facilities Management Companies?

Facilities management businesses need to ensure operational continuity, maintain aging infrastructure, merging legacy buildings and workplaces, and improve overall reliability and efficiency. Here's how IoT can be a game-changer for FM companies:

#### 1. Cost Reduction And Improved Efficiency

IoT enables FM managers to streamline operations through continuous planning and monitoring of maintenance. While it's nearly impossible to avoid maintenance and repairs, you can do a much better job with the help of a predictive maintenance feature.

Predictive maintenance, also called the holy grail of maintenance, is much easier to accomplish with the help of IoT. It uses the power of data to identify the potential breakdown before it even occurs. This allows you to act before failure takes place and increase asset performance. When Boeing put the predictive maintenance feature at work, they achieved almost 13% savings on the annual operational budget.

Secondly, IoT-enabled sensors can also help you optimise the way office space is being utilised. Based on the real-time data, you can provide better space management services and better schedule maintenance activities (check out the examples in the Use Cases section).

#### 2. Enhanced Safety And Security

IoT can significantly enhance security and emergency procedures. It can improve the physical security of a building or workplace by allowing communication between sensors, security cameras, alarms, implanted tags, and so on.

If any dangerous situation takes place, the pre-programmed sensors will send an automatic alert to first responders, and the occupants of the building. Sensors will prevent shutting down elevators during emergency situations and light up the exit passages.

Such type of functionalities reduce the risk of injury and improve the overall safety of the workplace.

On top of being beneficial, these smart security sensors are cost-effective too. According to the report, IoT security applications can reduce labour costs by almost 20%-50%. That's a considerable saving every year.

#### 3. Reduction In Expenses On Utility Costs

The cost of water, electricity, and natural gas usage is usually high compared to other utilities. Being a facilities manager, you can leverage IoT and cloud-based analytics to find out the pattern of usage and find ways to improve the efficacy.

According to McKinsey research, IoT-enabled energy monitoring can help save up to 20% of energy consumption and cost. The electric supply to the office can be integrated with IoT-enabled sensors. During the low supply and high-consumption periods, the grid will automatically switch to renewable energy, such as solar panels. The smart electric

grid can even gather data from different components and optimise the delivery on its own.

**4. Improved Well-being**

Today, business organisations are much more concerned about the well-being of their employees. IoT-enabled smart sensors can reduce the risk of work-related illnesses and injury. The sensors can monitor and automatically adjust the indoor environment to meet the needs of employees.

Occupants can set their preferences, and sensors will keep monitoring and improving the humidity and temperature of the space. Sensors will also monitor noise pollution or drop in air quality and make changes to ensure a fresh and healthy environment in the office.

These smart sensors can track the employee's posture and physical activity as well. If the employee is sitting on the desk for longer, it will adjust the seat to improve posture.

**5. Improved Stock Management**

Managing and maintaining the consumables stock is a recurring task for facilities managers. IoT can be a real saviour here. Different devices or machines like printers, refrigerators, etc., can be loaded with IoT-enabled sensors. These sensors will keep an eye on current stock and refill themselves when the stock is low.

## Use Cases Of IoT In Facilities Management

IoT systems can handle the majority of operations in the FM, especially the ones that are manually intensive and have low margins. Let's check out some of the best use cases of IoT in facilities management:

**1. Meeting Room Monitoring**

Occupants do not efficiently utilise meeting rooms – it is a common concern amongst all the facilities managers out there. Collecting the data about the current usage levels can help FMs make necessary changes to improve the efficiency of the meeting rooms. Sensors can collect data such as room temperature, humidity, and the number of participants in each meeting room.

*Designed by mindandi / Freepik*

Based on the data, the system will automatically adjust the room temperature, humidity, noise, and overall power usage required for the number of people. An optimisation of this level can help FMs save a considerable amount of energy.

Another smart application of IoT in the meeting rooms is the automatic alerts. Once the meeting room is vacated, the sensors will alert the cleaning department to make it ready for the next meeting.

**2. Hot Desk Management**

You can install the 'presence sensors' on each desk so people can remotely check whether there are any empty seats available for booking in real-time.
You can also use sensors to automatically cut down the power supply to the unoccupied desk area to save energy.

**3. Office Stationery, Consumables Stock Management**

Smart sensors can be installed on printers or refrigerators that will notify you in advance when the supplies are running low.

Printers integrated with Amazon DRS will automatically order new ink cartridge, and the fridge in office will automatically restock itself when the snacks are depleted.

**4. Washroom Usage And Cleaning Management**

Cleaning is one of the high volume activities and generally has low margins in the FM contract. Therefore, it's crucial to increase efficiency and reduce the cost of cleaning activities.

You can install motion sensors on washroom doors to approximate the washroom usage. The data would allow you to provide responsive cleaning services, improve the quality of service, and make efficient use of the cleaning staff's time.

You can configure the system to send alerts to the cleaning department after a particular number of uses. For example, the sensors will send alerts to the cleaning staff for washroom cleaning after every 100 users. There are many more examples of how IoT can be used in FM to improve the end-user experience and RoI.

## How To Evaluate Business RoI With IoT In Facilities Management?

When it comes to implementing IoT in facilities management, choosing the right IoT solution provider can have a significant impact on the ROI.

**Today, business organisations are much more concerned about the well-being of their employees. IoT-enabled smart sensors can reduce the risk of work-related illnesses and injury. The sensors can monitor and automatically adjust the indoor environment to meet the needs of employees.**

You need to partner with a company that has enough experience in scalability.

With the experienced IoT solution partner like Imaginovation, you can expand the initial IoT setup to different floors and add more smart services to your portfolio as your business grows (I am the co-founder and CMO at Imaginovation).

Make sure you have set the goals in your mind and what you want to accomplish with an investment in IoT. Ask yourself the following questions.

- What am I trying to solve?
- Is IoT the answer to my problem?
- How much would this save me compared to traditional solutions?
- Understand what specific problems you want to solve with the implementation of IoT.

For example, let's say you want to improve the efficiency of the air conditioning system in your facility. In that case, ask yourself whether you want the AC units to adjust the room temperature automatically, or you also want ACs to switch to renewable sources during low power supply or peak times.

Will the additional features like fault detection system beneficial for you? Make sure you know where precisely the finish line is before starting the race.

IoT has a multitude of applications in the facilities management business. If implemented correctly, it can provide a competitive edge to your business and help you stay ahead of the competition.

*Designed by Creativeart / Freepik*

# Check Point Software Fast Tracks Network Security With New Security Gateways

*New Fast Track Network Security's suite of solutions delivers highest-calibre threat prevention, on-demand Hyperscale expansion and unified security for enterprises of all sizes.*

Check Point® Software Technologies Ltd. a leading provider of cybersecurity solutions globally, has announced Fast Track Network Security, a new suite of solutions which deliver unprecedented protection, scalability, and ease of deployment and control for enterprises, from branch offices to corporate data centres.

According to the 2019 IBM Cost of a Data Breach study, the lifecycle of a malicious attack from breach to containment averages 314 days, and costs organisations $3.9M on average. Check Point Fast Track Network Security directly addresses the three main security challenges facing enterprises today: lacking a full set of security technologies to protect against advanced Gen V cyber-attacks; an inability to quickly scale up security according to business need; and complex, disjointed security management processes.

"Security breaches continue to impact enterprises across the globe at an alarming rate. The cost of a breach continues to rise as attackers have become more efficient, causing more damage in less time. Businesses need agile cybersecurity solutions that actively prevent breaches before they can cause disruption," said John Grady, Senior Principal Analyst from the Enterprise Strategy Group (ESG). "Check Point's continuing innovation around threat prevention and performance provides on-demand scalability, enabling enterprises to stay ahead of the attack landscape while meeting the changing needs of the business."

The Fast Track Network Security suite features five new Check Point Quantum Security Gateways™ for branch office to mid-size enterprises, and one gateway designed for Maestro Hyperscale orchestrations for large enterprises and data centres. All the gateways feature Check Point ThreatCloud and its award-winning SandBlast™ Zero-Day Protection. The new range starts with the 3600 gateway for branch offices, and extends to the 16000 Turbo Hyperscale gateway for enterprise data centres. All the Fast Track Network Security solutions include the latest release of Check Point's R80 unified security software, R80.40 which has over 100 new features to extend protection, streamline processes and enhance productivity.

"The principle behind Fast Track Network Security is simple. It enables enterprises to deploy the industry's leading threat prevention capabilities at all points of their infrastructure, and to scale security almost infinitely according to their

**According to the 2019 IBM Cost of a Data Breach study, the lifecycle of a malicious attack from breach to containment averages 314 days, and costs organisations $3.9M on average. Check Point Fast Track Network Security directly addresses the three main security challenges facing enterprises today: lacking a full set of security technologies to protect against advanced Gen V cyber-attacks; an inability to quickly scale up security according to business need; and complex, disjointed security management processes.**

changing business needs. It also dramatically accelerates the efficiency of their security operations," said Itai Greenberg, VP Product Management and Product Marketing at Check Point. "This enables enterprises to prevent and block even the most advanced attacks, before they can disrupt business."

### New Higher Performance, Power Efficient Gateways

The new Fast Track Network Security series of gateways all deliver over 2x the performance and half the energy consumption of rival high-end appliances. The range includes:

- 3600 Quantum Security Gateway for branch offices, offers up to 1500Mbps of threat prevention performance
- 6200 Quantum Security Gateway for small enterprises, with up to 2500Mbps
- 6600 and 6900 Quantum Security Gateways for mid-sized enterprises, with up to 7.6 Gbps
- 16000 Quantum Turbo Hyperscale Gateways for large enterprises with up to 17.6 Gbps

All of the gateways deliver a 100% block score for malware prevention for email and web, exploit resistance and post-infection catch rate, as seen in the NSS Labs' recent Breach Prevention Systems (BPS) Group Test.

They also feature lightning fast SSL-encrypted traffic inspection for maximum security and are Hyperscale-ready, capable of scaling up to 1.6 Tera-bps of Threat Prevention performance. The appliances are also equipped with dual, enterprise grade SSD storage and deliver faster processing with optimal CPU utilisation based on dynamic workloads technology.

### R80.40 Simplifies And Automates Security

R80 is the industry's most advanced threat prevention and security management software for data centres, cloud, mobile, endpoint and IoT. The newest R80.40 software release has over 100 new features, including zero-touch deployment capability that enables new security appliances to be set up and running within five minutes, and support for Check Point IoT Security which automates policy enforcement for IoT devices.

By consolidating all aspects of enterprise security environments seamlessly, R80 gives enterprises full visibility into security across their entire network fabric in a customisable visual dashboard, enabling them to manage the most complex environments easily and efficiently directly from their web browser.

Fast Track Network Security's combination of advanced new Quantum Security GatewaysTM, Maestro Hyperscale technology and the innovations of R80.40 software gives Check Point customers the quickest route to achieving Hyperscale network security with tera-bit levels of threat prevention performance, while accelerating and simplifying management processes.

# Commercial Applications For Cutting-Edge Intrusion And Alarm Tech

*Market and take advantage of these capabilities to expand the value of security systems in the retail, bank, school, and office verticals.*

By Tom Mechler, Regional Marketing Manager for Bosch Security and Safety Systems

Commercial applications share many similarities – they have multiple access points, times when the buildings are open and closed, people who need to be protected, and some level of risk day and night.

Despite the similarities, there are also many differences depending on the type of application. For example, retailers, banks, schools and office buildings all share a need to secure their facilities, but their specific pain points and risks differ. Integrators should build trust with customers by showing them you understand their needs and have the right-fit solution to improve their security and facility control.

The vertical market-specific examples all use the intrusion system as the heart of a commercial solution that increases security and makes systems easier to use. They demonstrate some of the many ways that integrators can sell customised solutions that address common needs in different vertical markets. By speaking the customer's language and knowing the challenges, dealers and integrators can deliver solutions that bring additional value to the customer, while driving increased revenue for their own businesses.

**Retail**

While a standard intrusion system in a retail store protects the premises when the store is closed, more advanced capabilities can help to protect interior areas, even when the store is open.

For example, help customers ensure that jewellery cabinets, gun or ammunition storage, or other high-value merchandise is protected – even when the intrusion system is disarmed – by adding a contact on the cabinet or case. The contact will enable the intrusion system to monitor how long that case has been open. Delaying the reaction of the point for a specified time – such as one minute – enables store personnel to be alerted to an abnormal condition via a text message or chime that reminds them to close and secure the case or cabinet before a report is sent to the monitoring station.

This same capability can apply to protecting schedule II narcotics in a retail store's pharmacy area, ensure a loading dock or cash room door is not left open, or alert to a perimeter door that is propped open.

In grocery or big-box stores, monitoring critical systems unrelated to security – such as refrigerated cases and freezers – adds significant value for a customer. If the temperature in a case rises above a certain threshold for

Designed by mrsiraphol / Freepik

longer than a pre-defined time, the retailer must dispose of the food, resulting in significant loss. The intrusion panel can connect to the systems that monitor temperature and provide a report, send a text, or play a chime to alert store personnel if action is needed to maintain the integrity of the stock, prevent spoilage and reduce loss.

For electronics stores, tightly-controlled stock such as mobile phones and tablets are often stored in a secured cage off the retail floor. Systems that combine intrusion and access control with disarm authority can help these customers protect that merchandise. For example, the system can limit access to ensure a manager is present before the cage can be opened. While employees may have the authority to unlock and disarm the store, the cage remains secured until a manager presents his or her token.

These system features provide added security and convenience for retailers – helping them go about the daily business of serving customers without burdening them with extra requirements for maintaining security.

The system can also extend beyond security to improve health and safety. For example, by integrating the intrusion control panel with IP cameras equipped with built-in video analytics, the cameras can trigger the panel to send a notification to store personnel if an object, such as a pallet of merchandise, is blocking an emergency exit. This improves safety for customers and employees.

**Banks**

Most banks have areas – such as an ATM service room – that should only have temporary access. By programming the area to re-arm automatically after a pre-defined time, the room is never left unsecured for a lengthy period, even

esigned by rawpixel.com / Freepik

if an employee servicing the ATM forgets to re-arm it. This feature can also secure vault rooms.

Vaults and other high-security areas within a bank may also require two people to enter their passcodes before disarming. Two-person disarm provides added protection. After the first passcode is entered, the system will prompt for a second code.

The intrusion system can also help to protect the branch manager if he or she is alone when opening the branch. By programming the system to require a passcode to be entered twice within a specified time period, banks have an added layer of security. The manager enters a passcode upon arriving, inspects the facility, and then enters the passcode again to disarm the system. If the manager does not enter the passcode twice within the pre-determined


Designed by fanjianhua / Freepik

time, the control panel will generate a duress event to the monitoring centre. With this feature, the branch manager has peace of mind that if an ambush attack occurs, a signal will be sent.

In addition, bank branches often use a secret signal to inform employees that it is safe to enter the branch. This signal may be opening a specific blind or turning on a specific light. The intrusion system can be programmed to automate this when disarmed by controlling other equipment or appliances.

## Schools

In schools, not every perimeter door has access control or an electronic lock – some are simply controlled with a traditional lock and key. These points can be monitored even when the security system is disarmed. If the door is propped open, the system can send an alert via text to the maintenance manager or principal to prompt them to close the door, ensuring a safer environment.

Technicians can also program the system to function differently if it is armed vs. disarmed. For example, if an emergency door is used when the system is armed, an alarm is sent to the monitoring centre. If the system is disarmed, a local alarm, such as a noise or siren, can alert

Designed by Freepik

the user. This ensures people within the building know that someone has used the door without resulting in a police dispatch. For added convenience, enable authorised staff to silence the siren using a wireless key fob instead of at the keypad to reduce unnecessary distractions for students in classrooms.

Controlling areas within the facility enables certain locations in the school – such as the gymnasium or auditorium – to remain disarmed while the rest of the building is secure. This provides flexibility to accommodate special evening


Designed by Freepik

or weekend sporting or performance events or even community meetings. Customisable functions can enable easy arming for these events with a single action or by presenting access credentials.

### Office Buildings

Limit access to sensitive areas of an office building, such as an IT room, using intrusion technology integrated with video and access control. These technologies combine to provide enhanced security and can even protect the individual hardware racks inside the room.

For example, each server rack can have its own access reader, keypad and camera. This can keep unauthorised individuals from accessing the equipment and restrict authorised people to scheduled days and times, limiting after-hour access to pre-determined times for maintenance or upgrades. Using a keypad and a reader on the racks also enables the use of dual authentication, so the individual must present something he or she has (credential) along with something he or she knows (a PIN) for even greater security. Adding the IP camera ensures that any attempts to open the racks by unauthorised individuals will trigger a text or email alert with a video snapshot to the facility manager.

The scheduling capabilities of the panel can also control the reaction of IP cameras integrated with the intrusion system, depending on time of day. For example, a person approaching the exterior of the building during the day when the system is disarmed will not trigger a camera action. However, when the system is armed at night, motion detected by the camera can fault a point on the control panel. This can prompt the panel to send an alarm verification event to the monitoring centre, trigger a light to turn on or a message to play over a loudspeaker, while sending a video snapshot to the facility manager.

*Designed by fanjianhua / Freepik*

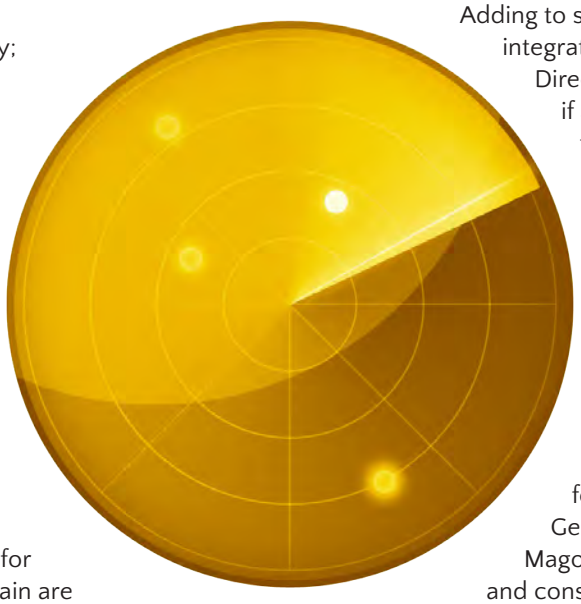
# Tech Trends: Put Radar on Your Radar

*The top six threats for this year revolve around IoT, cloud, ransomware, 5G, privacy and election security.*

**By Ray Coulombe, Founder and Managing Director of SecuritySpecifiers and the CONSULT Technical Security Symposium**

Over the last couple of years, I have begun hearing about the increasing use and availability of ground-based radar (GBR) systems applied to area intrusion protection. Recently, Terry Harless, a senior security consultant with 1898 & Co. (a recently formed entity within Burns and McDonnell), piqued my interest, so I decided to take a deeper look.

GBR systems use microwave energy; however, do not confuse that with microwave sensors. There are many microwave-based sensors designed for internal intrusion protection and certain outdoor systems, but outdoor system applications are best suited to perimeters and fence lines.



Radar brings to mind weather forecasts and aircraft control – just as these radars provide area scans, so do GBRs. "These systems work best in large unobstructed areas, such as open fields, and they are a good solution for night-time use and where fog and rain are of concern," Harless says. "IR thermal camera back-up adds to system effectiveness."

Radar systems work on reflected energy, and areas normally contain various elements that reflect energy back towards the radar. In the steady state, this is known as "clutter." An individual sweep of the radar may yield a reflection that stands apart from the clutter, which may be something of interest when seen on multiple consecutive sweeps.

Radar units are placed to detect a person or object moving radially toward or away from the sensor, triggering a change in frequency – known as the Doppler effect – and the primary basis for detection. Potential targets in motion tangentially (maintaining constant distance from the radar) or slow-moving objects may compete with high clutter levels and render detection more difficult.

Adding to system effectiveness is the integration of analytics into the system. Direction of motion rules will determine if a person or object is moving toward the sensor, allowing the system to alarm only upon motion vectors of interest. Stopped or slowing down vehicles may also be reasons to alarm. Discrimination between animals and humans or vehicles and humans further helps reduce false alarms.

"In the past two years, we are seeing huge increase in demand for GBR," says Yaron Zussman, General Manager of radar supplier Magos Systems. "Both end-users and consultants have realised that the improvement in sensor technology, radar software and reduction of cost make GBR a viable solution for many different verticals past the traditional defence applications. I expect machine learning and AI to accelerate this trend and to increase usefulness and reliability."

Harless says his primary application area to date is electrical utility substations, with priority given to critical substations

in the transmission network. "300 meters is about the farthest distance someone could shoot and cause damage to critical equipment within a substation, so we set these systems to detect up to 500 meters and in some cases further, depending on the landscape, to allow adequate reaction time," Harless explains.

Other interesting applications include airports, data centres, prisons, campuses and industrial complexes – all areas with likely large open spaces around them – and drone detection, where timing of deployment remains uncertain due to FAA rules.

### Technical And Other Deployment Considerations

An important consideration is FCC licensing. Certain systems work in the ISM band and may be able to operate unlicensed. The resulting advantage of speedy deployment may be offset by the presence of other systems broadcasting in the same band. Licensing may create project delay and add cost but help assure a more favourable signal environment.

Harless sees the closest competing technology being thermal cameras, with a sensing distance crossover point of approximately 100-200m, where GBR provides a cost advantage. However, PTZ cameras – thermal or IR assisted – are normally used in conjunction with GBR to verify the object being detected. A single GBR can cover enormous swaths of land while cameras typically have a narrow angle of view when used for long distances.

"Correct deployment is the key to successful operation," says Brock Josephson, Physical Security Consultant and a colleague of Harless at 1898 and Co. "It is sometimes difficult to anticipate factors that could decrease performance, such as high levels of reflected power – too much of which

**Radar systems work on reflected energy, and areas normally contain various elements that reflect energy back towards the radar. In the steady state, this is known as "clutter." An individual sweep of the radar may yield a reflection that stands apart from the clutter, which may be something of interest when seen on multiple consecutive sweeps.**

*Designed by Freepik*

can saturate the receiver. When possible, testing onsite, in advance of deployment, can help identify these and other difficult to anticipate issues."

Key considerations when deploying radar include: avoidance of obstacles and creating blind spots; clear line of sight; positioning to detect radial movement; clutter reduction; and avoidance of reflective objects, such as metal, glass, etc.

### Choosing A Solution And Partner

For consultants and integrators alike, GBR represents a proven and useful technology that should be in the mix for consideration for wide area sensing, particularly beyond 100 meters. When comparing and choosing products, here are some of the primary comparative factors:

- Vertical and azimuth – think of vertical and horizontal field of view. A higher vertical number provides extra margin for look down from the radar unit. Typical field of view is 100-120 degrees horizontal, and 20-30 degrees vertical, providing the potential to cover hundreds of acres.
- Distance – published distances will vary for vehicles (longest), humans and even drones. GBR systems are advertised with distances up to 13 km for vehicles, 800 meters for humans and 500 meters for drones.
- Range resolution – a measure of location uncertainty.
- Licensed vs. unlicensed.
- Power – emitted power and consumed power.
- PoE operation – potentially simplifying deployment and saving installation cost.
- OEM integrations – operation tightly integrated with video systems increases overall system effectiveness.
- Cost

# Lidar Comes Of Age In Security

*Industry experts discuss how the technology has evolved and where it is headed in the market.*

**By Joel Griffin, SecurityInfoWatch.com**

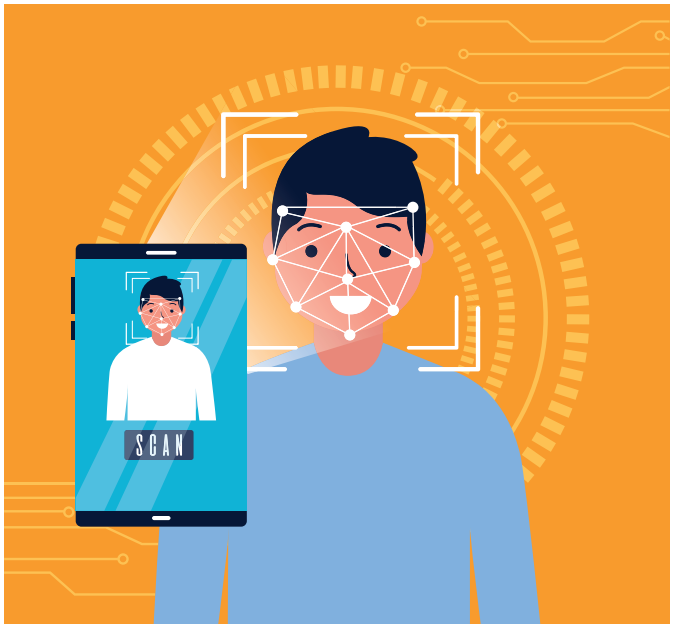
With all of the technological advancements taking place across the security industry these days, it's easy for some solutions to get lost in the shuffle. From machine learning and advanced video analytics to facial recognition systems and robotics, the market seems awash in products that promise to revolutionise day-to-day security operations for organisations both big and small.

One technology that has flown under the radar among these other industry innovations is light detection and ranging, known as lidar, for short. Lidar solutions leverage lasers to measure reflected light off of objects to create a 3D image of an area. The technology, which is known primarily for the vital role it plays it in autonomous vehicle development, also holds enormous potential for security applications.

Unlike a surveillance camera that measures ambient light and captures associated images, Derek Frome, Director of Marketing for Ouster, which is showcasing its OS-1-64 Lidar and Object Tracking sensor at this year's GSX conference in Chicago (Booth #1976), lidar is an active illumination sensor that sends out light (laser pulses) enabling users to reconstruct an environment in great detail.

"Based on the speed of light, we can tell exactly how far away something was and so you can imagine across 1.3 million data points per second, you can get a very high-resolution 3D creation of an environment. Whether it is daytime or night-time, it doesn't matter," Frome says.

According to William Muller, Director of Business Development at Cepton Technologies, which is exhibiting for the first time at GSX this year (Booth #1894), lidar provides a wealth of information about a given




Designed by gstudioimagen / Freepik

environment – i.e. size, direction and velocity of objects – within centimetres of accuracy that just isn't possible with other technologies.

"One differentiator for lidar compared to other technologies is that we have zero emissions. Radar and microwave (technologies) emit frequencies of some sort, while fibre optics emit only light but it is not as accurate. And, of course, we are all used to video-based images – thermal or megapixel cameras – but a lot of those devices struggle to position an object in the field of view to say that that object is 10, 15 or 20 meters away," Muller explains. "For lidar, however, it is easy to say that an object is, for example, 55 meters away, and then take another available resource like a PTZ camera and it can give accurate information

**With all of the technological advancements taking place across the security industry these days, it's easy for some solutions to get lost in the shuffle. From machine learning and advanced video analytics to facial recognition systems and robotics, the market seems awash in products that promise to revolutionise day-to-day security operations for organisations both big and small.**

to say that target is something of interest. It's really an old technology being modified for new world challenges. Especially in security, there hasn't been a lot of new, innovative hardware… so this just adds that next layer of proactive threat detection."

### Differences In Lidar Offerings

What separates Ouster, which received the 2019 GSX Innovative Product Award in the "Judge's Choice" category for the aforementioned OS-1-64 sensor, from other lidar vendors, according to Frome, is the resolution offered by their sensor which today stands at 64 channels.

"A 64-channel sensor is easily human-readable," Frome says. "You can tell a person from quite a way away, you can tell animals, vehicles or whatever it is. The other half of the coin is the price. We have a very aggressive price point in the market which really allows us to even be considered for applications like security. A lot of lidar companies are selling sensors for $30,000 to $100,000 each and the cost-benefit analysis gets thrown pretty out of whack for a use case like security when talking about a sensor that costs tens of thousands of dollars. Our 16-channel sensor is $3,500 and our 64-channel sensor is $12,000 in single-unit quantities and obviously we are able to offer discounts for larger purchases."

Realising that high-resolution lidar would need to migrate away from traditional analogue components to a semi-conductor-based supply chain to be leverage in autonomous vehicles and other applications, Frome says Ousters founders set out to develop the world's first digital lidar sensor.

"That's really what we've been working on and the products we've launched basically take what would be a many thousands of components analogue device and we condense it down into two integrated semiconductor chips," he explains. "We have a laser array on one chip and a receiver called a SPAD (single-photon avalanche diode), which is a CMOS sensor similar to digital photography, on the other.

"It's a very different technology, a totally different supply chain and what it allows us to do is really deliver that high performance," Frome continues. "Similar to how Intel ships a processor every year that is about twice good and also has cost reductions, we have a similar situation where last year we brought out the OS-1-64, which has 64 lines of resolutions and this year we're bringing out the 128-channel sensor. We see that trend continuing for many years to a point where we have lidar that you can truly call HD and that gets interesting for a lot of different industries, security included."

Whereas lidar solutions are still in the development stages within many companies, Muller says Cepton is one of the few to bring an actual solution to the market.

"A lot of the other lidar manufacturers are just focused on making sensors but we've developed the whole package," he says. "We're taking that lidar data and we are presenting usable information with what that technology is seeing and that is the classification and detection of these objects or potential threats being human or a vehicle, etc."

### Integration With Other Security Systems

In addition to presenting its solution to the market, Cepton has also announced a new partnership with CNL at GSX. Under this new partnership, Cepton's smart lidar network, Helius, will be integrated with CNL's PSIM software to enable automation of threat detection, tracking, and escalation in real-time.

"The core of Cepton's design is very open source so we are driving a partner ecosystem model. We want to allow as many partners and other systems to receive our information," Muller adds. "I wouldn't say we are a total solution, but we offer a layer that goes a long way in providing that full solution."

While Ouster hasn't integrated its lidar sensor with any other security hardware or software solutions on the market, Frome says that some installers have integrated their technology with camera systems and other products, such as proximity alarms and things along those lines.

"The data that comes off of (the sensor) is just raw data so you can do all sorts of machine learning, perception algorithms on top of the sensor data as well," he adds.

# Intrusion And Access Control: The Perfect Pair For Facility Security

*When incorporating the security of a business, a multi-layered approach to technology can go a long way in safeguarding critical assets, including employees and visitors.*

By Ross Wilks, Head of Marketing Communications, Vanderbilt/ComNet

Integration is the name of the game for today's enterprise facilities. Whether they're looking to streamline entry for visitors and staff or leveraging event management software to ensure access to specific parts of a facility, facilities managers must take a number of considerations from a technology standpoint into account.

Most facilities leverage video surveillance technology in an effort to capture the comings and goings of staff and guests. Video is perfect for providing forensic evidence in the event of an incident, but without additional integrated platforms to help pinpoint problems, video can fall flat. That's why it's critical for a facility to also incorporate the use of intrusion and access control platforms to increase situational awareness and shift from a reactive response to a more proactive approach.

The benefits of melding intrusion and access control within a facility's infrastructure are numerous.

**Increased Connectivity**
Within intrusion and access control, there's certainly a trend among facilities toward all devices becoming smarter, interoperable and interconnected, especially with the rise of the Internet of Things (IoT) and the data being generated from various connected devices.

Facility managers demand the ability for their intrusion detection system to work seamlessly with and talk to their access control system, in addition to fire detection and video management systems. Doing so allows the right information to be gathered when it's needed most in an effort to protect a facility and its occupants.

**More Communication**
With increased levels of connectivity comes the demand from facility managers to enhance communications across devices and teams. There are a number of new wireless initiatives across the security industry that are

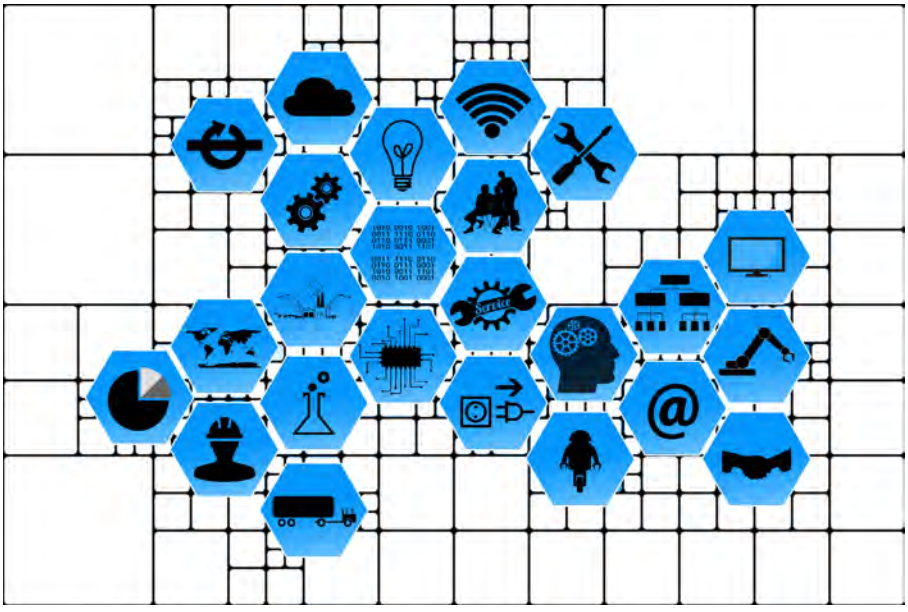


*Image by Gerd Altmann from Pixabay*

designed to bring two-way communication to the forefront through a cloud-based system that utilises the same interface but can be programmed either onsite or remotely. This is a powerful tool for installers that has already gained popularity. When an intrusion platform can communicate directly to and from an access control platform, operators are better able to see all of the information they need at any given time. For example, when a door is pried open or a reader is compromised, an alarm can notify an operator and ensure all of the information is communicated for an appropriate response.

**Streamlined And Remote Management**

The Internet has remarkably revolutionised the way technology is used, allowing organisations to create an extension of systems and processes that once required a plugged-in setup to mobile devices. The ability to remotely manage and monitor a facility is paramount to achieving the kind of flexibility that facility managers want today, combining ease of use, efficient response abilities and centralisation to deliver higher levels of situational awareness. For example, any time an intrusion alarm goes off, remote monitoring and management make it possible to investigate the alarm from anywhere, on any device and at any time. This makes response times faster, allowing greater protection for facilities.

**Shift From Reactive To Proactive**

Integrating access control and intrusion can help operators determine whether risk to a facility is imminent. Factoring in the time of day for regular access and being able to set up alerts when a building is accessed outside of those hours (for example, by someone who has copied a key card) can allow operators to determine whether there is a potential breach or investigate the reason for someone accessing the building. This approach helps an organisation remain vigilant on a regular basis. The integration of the two systems can also allow facilities managers to set specific access levels based on an employee's role, further tailoring a solution to fit a company's needs.

**Facility managers demand the ability for their intrusion detection system to work seamlessly with and talk to their access control system, in addition to fire detection and video management systems. Doing so allows the right information to be gathered when it's needed most in an effort to protect a facility and its occupants.**

Incorporating intrusion and access control into a facility's overall security plan is not only recommended, it's essential to protect people and assets on a day-to-day basis. An integrated, multi-layered approach can help deliver 24/7 protection that can increase overall situational awareness across a facility and streamline response.

*Designed by Pressfoto / Freepik*

# Tech Improves Remote Guarding And Monitoring

*New video verification technologies are enabling integrators to address previous issues and create a more reliable solution.*

**By Daniel Gundlach, General Manager and VP of Security for FLIR Systems**

Airports, utilities, data centres and other mission-critical sites all occupy vast amounts of land. Detecting and deterring threats across these large properties is paramount to the successful operation of these enterprises.

If vulnerable to intrusions, critical infrastructure facilities will be subject to loss and business interruptions that can affect thousands of people. In the United States alone, the Associated Press reported 345 breaches from 2004 to 2016 at 31 major airports — many of which resulted in costly damage to property, as well as the disruption of air traffic procedures.

To improve perimeter security, many large enterprises have employed remote video monitoring, or the use of video cameras and analytics to survey the property and notify the appropriate personnel of any intrusions. Event-based video has been a force-multiplier for many businesses and has helped to create strong interest in remote guarding systems, which connect surveillance cameras, sensors and analytics to monitoring centres with security operators acting as virtual guards.

Together, remote monitoring and guarding offer expanded coverage and greater efficiency. Instead of a security officer having to physically patrol an entire property or stare at a video wall in a command centre, they can be alerted to a specific event in a designated area that may require a response.

Traditionally, however, these remote monitoring and remote guarding solutions have carried with them a predicament of their own. To many customers' surprise, these systems produced a relatively high number of false alarms – mainly due to the relative infancy and imprecision of video analytics. Fortunately, there are strategies and

**To improve perimeter security, many large enterprises have employed remote video monitoring, or the use of video cameras and analytics to survey the property and notify the appropriate personnel of any intrusions. Event-based video has been a force-multiplier for many businesses and has helped to create strong interest in remote guarding systems, which connect surveillance cameras, sensors and analytics to monitoring centres with security operators acting as virtual guards.**

technologies today that are helping integrators address these issues and offer their customers a more reliable remote monitoring and guarding solution.

### The Pesky Problem Of False Positives

According to the 2016 Resolutions of the International Chiefs of Police, 98 percent of all alarms are false. Case in point – in 2016, the Memphis Police Department responded to 62,494 alarm calls where just 458 were true events. About 51 percent of these alarm calls came from commercial properties.

Wildlife, moving foliage, wind, insects, low-performing sensors and human error are all common causes of false alarms. False alarms are expensive and also time-consuming. In 2016, the Memphis Police Department spent $1.7 million allocating resources to respond to false alarm calls, which consumed 63,952 hours of officer time; however, it is not just law enforcement losing time and money answering false alarms. Enterprises are also wasting resources dispatching guards to investigate alerts that turn out to be false positives.

All of these factors have contributed to a lack of confidence in remote monitoring systems and video analytics from integrators, end-users and law enforcement alike.

To mitigate the issue of law enforcement officers repeatedly responding to false alarms, cities like Memphis have begun to impose fines on companies and individuals. In Memphis, a user can be charged $140 when police respond and there is no true threat. Implementing fines has helped to curb the problem. The Memphis Metro Alarms Office reported a 20 percent decrease in false alarms after the fines ordinance was enacted in July 2017.

### Technology Rises To The Challenge

What nuisance alerts have truly revealed is the need to better verify an alarm before first responders are dispatched. Today, security technology manufacturers are offering much more refined technologies to address false alarms and optimise video verification. By integrating more refined technologies, these solutions are delivering more accurate alarms and lowering the total cost of ownership of remote monitoring systems.

Here are a few key strategies that are driving this movement of enhanced remote monitoring and remote guarding forward.

***1. Leveraging more advanced technologies:*** Innovation in product development has led security manufacturers to offer what were once military-grade technologies, such as thermal sensors and radar, at more accessible price points. As a result, these technologies are now being deployed in broader markets, such as commercial or industrial perimeter security applications. They are becoming more mainstream, and they are being integrated as specialty technologies in high-end, remote monitoring systems to enhance intrusion detection. Improved sensor technology increases the probability of an getting an accurate alarm.

***2. Enhanced video analytic performance with thermal:*** In particular, the integration of thermal sensors in remote monitoring solutions substantially improves threat detection and video verification. As thermal cameras do not require a light source to produce video, they enable 24/7 surveillance in the toughest conditions, such as fog, rain, mist and even total darkness.

Considering that nearly half of all burglaries occur at night, according to the U.S. Department of Justice, thermal technology adds significant value to remote monitoring solutions. Because thermal sensors create images by measuring the minute differences in heat signatures vs. light, they yield high-contrast, sharper images, regardless of the weather or lighting conditions. Thus, thermal images enable video analytics to perform optimally at all times.

Integrating thermal sensors with remote guarding solutions also improves video verification by providing another video stream for remote operators to observe and verify an alarm. The International Chiefs of Police defines a "verified alarm" as "an electronic security system event in which a trained central station operator utilising a standardised protocol has determined the presence of human(s) and the high probability that a criminal offense is in progress."

**The key objective for remote guarding systems is to use technology to allow remote monitors to engage suspects in real time and proactively deter crimes from being committed on the property. The integration of two-way audio capabilities in remote guarding systems is now a standard feature for live response, as this functionality allows guards to issue warnings or directives over bi-directional speakers.**

High-contrast thermal images enable central station monitors to easily distinguish a human hiding in the bushes, for example, whereas the night scene may not be as clear when observing a video clip from a standard surveillance camera.

***3. Improved threat assessment with HD:*** Now popular 1080p and 4K cameras are also improving image clarity and analytics performance in remote monitoring solutions. These HD cameras deliver evidentiary-class video, reducing the risk that video footage will be pixelated, blurred or hazy – thanks to their higher resolution. Built-in IR illuminators are also increasing the effective range of HD cameras at night.

All in all, these HD cameras are allowing central station monitors to see greater scene detail. The high-quality, full colour video clips are improving a remote guard's ability to identify suspect characteristics, giving them more specific information to share with law enforcement.

***4. The all-in-one solution:*** The concept of integrating multiple technologies – such as thermal sensors, analytics, visible cameras and illumination technologies – into one unit has made remote monitoring solutions more appealing. On a practical level, this reduces infrastructure and hardware footprint. On an applicational level, these turn-key solutions are proving more cost-efficient than older designs by housing all technologies within a single device.

These all-in-one solutions essentially reduce equipment and labour needed for installation, which ultimately lowers overall project expenses for integrators, positively affecting the bottom line.

Improving Live Response And Intruder Disorientation
Connecting remote monitoring systems to central stations via the cloud enables security operation personnel to actively monitor and guard sites as well as respond to incidents as they unfold.

The key objective for remote guarding systems is to use technology to allow remote monitors to engage suspects in real time and proactively deter crimes from being committed on the property. The integration of two-way audio capabilities in remote guarding systems is now a standard feature for live response, as this functionality allows guards to issue warnings or directives over bi-directional speakers.

Another tactic being deployed in remote guarding systems to delay intruders is incorporating white LED illuminators. Upon detection of an intruder, the LEDs act as a floodlight and flash to momentarily disorient the suspect. The bright white lights ultimately communicate to a suspect that their behaviour did not go unnoticed.

Deploying precise sensors that yield more accurate detection and enhanced video verification is a tried-and-true method to improve remote monitoring and guarding systems; moreover, using solutions that integrate multiple technologies with a track record of success in large perimeter applications under one housing is another best practice to simplify design layouts and increase efficiency.

At the end of the day, having a high-performing remote monitoring solution gives customers greater peace of mind and assurance of their security investment.

# Cyber-insurance Is On The Rise – And So Is Ransomware

A debate has erupted between the insurance industry and the infosec community over whether cyber-insurance payouts have led to the surge in ransomware attacks this year.

**By Rob Wright, TechTarget**

Which came first – the ransomware chicken or the cyber-insurance egg? That's the central question to a debate that has emerged in the wake of massive spikes in both cyber-insurance policies and ransomware attacks this year, as infosec professionals speculate about possible connections between the two.

On one side of the debate is the fast-growing cyber-insurance industry, an estimated $4-plus billion market that's experiencing massive growth. On the opposite end is the infosec community, which is grappling with a surge in ransomware attacks this year. While no studies have shown a direct connection between the rising number of cyber-insurance policies and ransomware attacks, the infosec community has grown increasingly concerned – and vocal – about a possible link.

The theory, according to infosec professionals, is that cyber-insurance policies give companies an easy and affordable way to pay the ransoms and retrieve their data, which in turn leads to more ransomware attacks. In a recent blog post titled "Cyber insurance: here to stay, whether we like it or not," Christopher Boyd, lead malware intelligence analyst at Malwarebytes, said ransomware helped "supercharge" the cyber-insurance market, which has facilitated the ransom payment process.

"At this point, it doesn't really seem to matter much if the victims pay up off their own back, if they hand over a ransom then reclaim money from insurers, or if the insurer is simply on hand to cover recovery and clean-up costs," Boyd wrote. "The bottom line is, it's hard to argue that this doesn't just keep the attacks coming."

The insurance industry, however, has pushed back on that line of thinking. In October, insurance brokerage Marsh published a report titled "Cyber Insurance is Supporting

the Fight Against Ransomware" that contested "misinformation" in the media about policies driving ransomware's growth.

"Far from being part of the problem, cyber insurance can be a valuable tool in the fight against ransomware and other cyber threats," Matthew McCabe, senior vice president and assistant general counsel for cyber policy at Marsh, wrote. "Fulfilling its traditional role, cyber insurance pools insureds that are similarly at risk and spreads their potential losses."

Still, security vendors claim they've seen an increase in the number of organisations that choose to pay the ransom, despite recommendations from law enforcement and infosec experts not to pay.

"We're getting into the area of speculation, but what impact has cyber-insurance had [on the increase]?" said Raj Samani, chief scientist at McAfee. "There are insurance companies whose default position is to pay. And actually, that's understandable."

For example, Samani said, if a major city has been crippled by ransomware and the ransom is $1 million but the downtime, restoration and clean-up costs are projected to be $100 million over several weeks, then it's easy to see why organisations would choose the former option over the latter.

Amid a string of high-profile costly ransomware attacks on municipalities and healthcare organisations, the debate suggests there's a growing chasm between the infosec and insurance industries.

Designed by rawpixel.com / Freepik

### A Symbiotic Relationship?

Ransomware has had a clear impact on the cyber-insurance market; many carriers say ransomware and business email compromise the two biggest drivers of claims this year.

But it's difficult to determine how much of an effect, if any, the cyber-insurance market has on the ransomware landscape. Insurance carriers and brokers don't publish the number of clients who pay to retrieve their data, and neither do security vendors that perform incident response on ransomware attacks.

Some vendors have published anonymous survey results that show the overall percentage of businesses that pay ransoms. For example, SentinelOne's 2018 Global Ransomware Report showed that 45% of U.S. businesses hit with ransomware chose to pay at least one ransom, though the survey data didn't explain what role cyber-insurance played in the decision to pay. Still, there are some things that both industries generally agree on; ransomware attacks and ransom payments are increasing.

"Ransomware certainly is the thing that, as an industry and a company, is having the biggest increase in terms of frequency and the severity of the event," said Tim Francis, enterprise lead for cyber-insurance at Travelers Companies, Inc. "And it's not just that the ransom demands are increasing – and they are."

In addition, Francis said ransomware attacks are generally more

sophisticated, and because of that the potential impact on an organisation's entire environment is much larger.

John Farley, managing director of the cyber practice group at insurance brokerage Arthur J. Gallagher and Co., agreed and said his company is "absolutely" seeing increases in terms of both frequency and severity.

"Just a few years ago, ransom demands were averaging between $5-$10,000," he said. "Now demands are typically in the six-figure range."

It's difficult to tell whether cyber-insurance has had an effect on the increase, Farley said, and there's no evidence that suggests attackers know if a target has cyber-insurance or what their coverage may be.

"I don't think cyber-insurance is necessarily driving this," he said, "but I do think [attackers] are measuring how many times someone's actually paying. And if you're getting paid, you're going to continue the crime."

### Cyber-Insurance Concerns

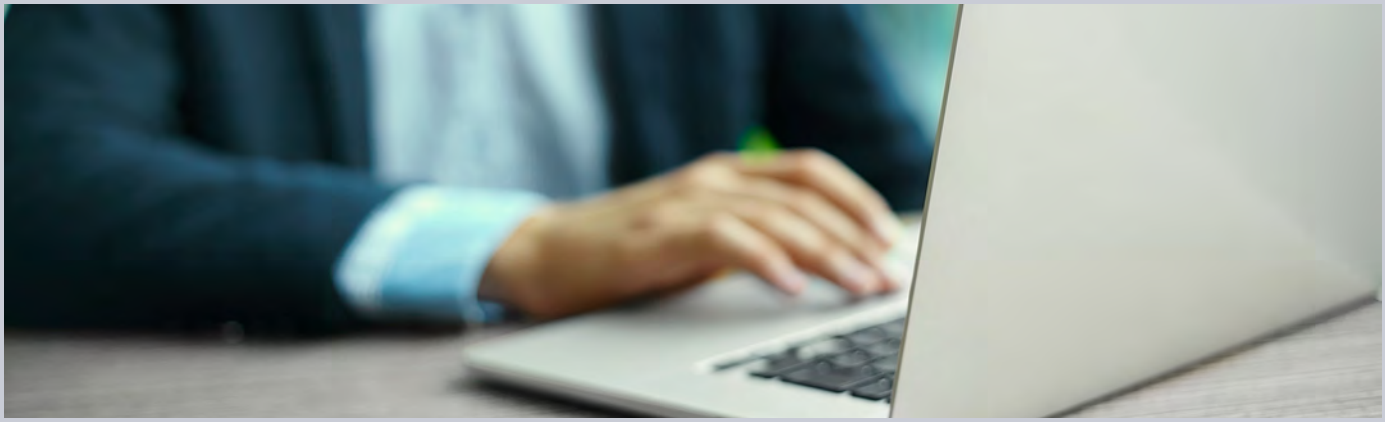
Despite the lack of a definitive connection, some security vendors suggest cyber-insurance contributes to the overall increase in ransom payments, which they claim indirectly contribute the overall surge in attacks.

For example, earlier this month anti-malware vendor Emsisoft noted in its "State of Ransomware in the US" report for 2019 that "Organisations that have cyber insurance may be more inclined to pay ransom demands, which results in ransomware being more profitable than it would otherwise be and incentivises further attacks."

> **"The one thing everybody is starting to become aware of is, if you have a ransomware incident and have almost any type of cyber liability insurance, then the insurance carrier is going to pay the ransom."**

Emsisoft did not release specific numbers about cyber-insurance or paid ransoms and said the report is based on observations from researchers within the Emsisoft Malware Lab. Emsisoft spokesperson Brett Callow said "it is impossible to say" whether more victims choose to pay ransomware demands.

But Callow also said cyber-insurance policy holders may be more inclined to pay ransoms "simply because the money does not come directly from their pockets. Additionally, in the case of the public sector, paying a $10,000 deductible may be more politically palatable than paying a $500,000 ransom."



Designed by hatoyalex / Freepik

To that end, Ryan Weeks, CISO at backup vendor Datto, said his company has seen organisations that ultimately choose to pay the ransom through their cyber-insurance carrier rather than pay to restore data from backups and replace encrypted systems, which can cost more.

"The one thing everybody is starting to become aware of is, if you have a ransomware incident and have almost any type of cyber liability insurance, then the insurance carrier is going to pay the ransom," Weeks said.

Weeks said there's an "almost inherent incentive in the insurance market to pay the ransom," but he also said it would unfair to blame cyber-insurance for the spike in ransomware attacks until a comprehensive study is performed to establish a cause and effect between the two.

But Farley said having a cyber-insurance policy doesn't necessarily mean the organisation is going to pay the ransom. "I think cyber-insurance can have the opposite effect," he said, explaining that a policy could allow an organisation to pay the costs of business interruption, lost revenue and data/asset restoration.

**To Pay Or Not To Pay?**

However, Farley acknowledged that some organisations, particularly state and municipal governments, can be under enormous pressure to restore their systems as quickly as possible. He pointed to the rise of ransomware attacks on major cities like Baltimore and Atlanta, which led to the U.S. Conference of Mayors to pass a resolution earlier this year that opposes paying ransoms because it "encourages continued attacks on other government systems, as perpetrators financially benefit."

"I think a lot of people agree with that," Farley said. "Number one, no one wants to perpetuate the crime, number two, you don't know who you're paying, and three, there's no guarantee you'll get your data back."

The other side, he said, is that municipalities may have to contend with emergency services being offline, which could potentially impact public safety, and could lead to higher overall restoration costs that will ultimately fall on taxpayers.

The debate over whether victims should pay or not isn't a simple one, Francis said. Insurance carriers like Travelers take all factors into consideration when advising clients, who ultimately make the final decision.

"Each situation is different. Sometimes it's better to pay the ransom, and sometimes it's not," he said. "Depending on how long an insured organisation is willing to go potentially with their systems down, it may be better to try to restore. But sometimes when you pay the ransom, it doesn't work as well as you think."

**Behind-the-scenes Payments**

Insurance carriers aren't the only entities that may be contributing to a higher rate of ransom payments. McAfee's Samani said there are a number of "ancillary services" that market data recovery but are actually just paying ransoms behind the scenes to retrieve customers' data.

"There's an entire ecosystem that's been created offering ransomware recovery services," he said. "There are those that claim to be able decrypt those ransomware variants that have no [publicly available] decryptors, so either they have the most amazing computing power the world has ever known, or they are in some way, shape or form paying for that decryptor."

It's unclear if ransomware operators incorporate cyber-insurance into their strategies, either to raise overall ransom demands or to specifically target insured organisations. But Weeks believes, given the amount of money that's at stake, that if it hasn't already happened, it soon will.

"At the end of the day, people are going to do whatever they have to do to get their businesses back up and running," Weeks said. "And the attackers know this, and so everything they do is designed to maximise the success of that ransom payment."

# How To Navigate A Ransomware Recovery Process

If you find your systems locked up from a ransomware attack, what should you prioritise? Before you start your recovery, follow this plan to avoid additional trouble.

By Brian Kirsch, IT Architect and Instructor at Milwaukee Area Technical College

If your defences and backups fail despite your best efforts, your ransomware recovery effort can take one of several paths to restore normalcy to your organisation.

Ransomware is bad enough. Don't rush to bring systems and workloads back online and cause additional problems. The first item on your agenda is to take inventory of what still functions and what needs repairs. This has to be done quickly, but without mistakes. Management will want to know what needs to be done, but you can't give a report until you have a full understanding. While you don't need to break down every single server, you will need to have everything categorised. Think Active Directory, file servers, backups, networking infrastructure, email and communication, and production servers to start.

### Take Stock Of The Situation

The list of affected systems and VMs won't be comprehensive. You have to start with machines that are a priority, and production servers are not in this case. If Active Directory is down, then it's a safe bet most of your production servers – and the IT infrastructure – won't be running correctly even if they weren't directly affected.

To start with a ransomware recovery effort, check your backups first before anywhere else. Too many folks have deleted encrypted VMs only to find the malware wiped out their backup systems and end up going from bad to worse. Mistakes happen when you rush.

A somewhat easy path of restoring servers does exist if your backups are intact, current and operational. The restoration process needs to be tested before you delete any VMs. Rather than removing affected machines, try relocating them to lower-tier storage, external storage or even local storage on a host. Your goal is to get the encrypted VMs out of the way to give yourself space to work, then try the restores and get the VMs running before you remove their encrypted counterpart.

### It Might Be Time To Make Difficult Choices

If the attack corrupted your backup system or the ransomware recovery effort failed, then someone above your pay grade will have to make some decisions. You will have to have a few difficult conversations, partly because the responsibility of the backups – and their reliability – rested on you. It's possible it's not entirely your fault for different reasons, such as not getting proper funding. This will have to be a conversation for a later time. At the moment, it's time to make a decision: Pay the ransom, rebuild the systems or file a report.

Reporting requires the involvement of senior management and the company legal team. If you work for a government entity or public company, then you might have very specific guidelines that you must follow for legal reasons. If you work for a private company, then you still have possible legal issues with your customers about what you can and cannot disclose. No matter what you say, it will not be taken well. You want to be honest with your customers, but you also need to be mindful and limit how much data you share publicly.

The other aspect to reporting involves the authorities. Your organisation might not even have been the intended target if you were hit by an older ransomware variant. If that's the case, it's possible there might be a decryption tool. It's a long shot, but something worth check before you rebuild from scratch.

While distasteful, paying the ransomware is also an option. You need to consider how much will it cost to rebuild and recover versus handing over the ransom. It's not an easy call

Designed by Freepik

to make because a payment does not come with any guarantees.

Most companies that pay the ransom typically don't disclose that they paid or that they were even attacked. I suspect most organisations get their data unlocked, otherwise the ransomware business model would collapse.

The challenge with rebuilding is the effort involved. There are relatively few companies that have people who fully understand how every aspect of their environments work. Many IT infrastructures are the combined result of in-house experts and outside consultants.

People install systems and take that knowledge with them when they leave. Their replacements learn how to keep these systems online, but that is very different from installing or building them from scratch. Repairing Active Directory is a challenge, but to rebuild an Active Directory with thousands of users and groups with permissions from documentation – with any luck – is next to impossible unless you have a lot of time and expertise.

Recovering from a ransomware attack is not an easy task, because not every situation is identical. If your defences and backup recovery fail, the reconstruction effort will not be easy or cheap. You will either have to pay the ransom or spend money in overtime and consultants to rebuild mission-critical systems. Chances are your customers will find out what is happening during this recovery process, so you'll have to have a communication plan and a single point of contact for the sake of consistency.

Ransomware isn't something just for the IT department to handle; the decisions and the road to recovery will involve several stakeholders and real costs. Plan ahead and map out your steps to avoid rushing into bad choices that can't be reversed.

# Ransomware Attacks Shaking Up Threat Landscape – Again

Threat actors have employed new techniques and built more sophisticated business models for their ransomware campaigns, which has had devastating consequences.

**By Rob Wright, TechTargetCollege**

Ransomware is changing the threat landscape yet again, though this time it isn't with malicious code.A spike in ransomware attacks against municipal governments and healthcare organisations, coupled with advancements in the back-end operations of specific campaigns, have concerned security researchers and analysts alike.

The trends are so alarming that Jeff Pollard, vice president and a principal analyst at Forrester Research, said he expects local, state and city governments will be forced to seek disaster relief funds from the federal government to recover from ransomware attacks.

"There's definitely been an uptick in overall attacks, but we're seeing municipality after municipality get hit with ransomware now," Pollard said. "When those vital government services are disrupted, then it's a disaster."

In fact, Forrester's report "Predictions 2020: Cybersecurity" anticipates that at least one local government will ask for disaster relief funding from their national government in order to recover from a ransomware attack that cripples municipal services, whether they're electrical utilities or public healthcare facilities.

Many U.S. state, local and city governments have already been disrupted by ransomware this year, including a massive attack on Atlanta in March that paralysed much of the city's non-emergency services. A number of healthcare organisations have also shut down from ransomware attacks, including a network of hospitals in Alabama.

The increase in attacks on municipal governments and healthcare organisations has been accompanied by another trend this year, according to several security researchers: Threat actors are upping their ransomware games.


Today's infamous ransomware campaigns share some aspects with the notable cyberattacks of 20 years ago. For example, the ILoveYou worm used a simple VB script to spread through email systems and even overwrote random files on infected devices, which forced several enterprises and government agencies to shut down their email servers.

But today's ransomware threats aren't just using more sophisticated techniques to infect organisations – they've also built thriving financial models that resemble the businesses of their cybersecurity counterparts. And they're going after targets that will deliver the biggest return on investment.

## New Approaches

The McAfee Labs Threats Report for August showed a 118% increase in ransomware detections for the first quarter of this year, driven largely by the infamous Ryuk and GandCrab families. But more importantly, the vendor noted how many ransomware operations had embraced "innovative" attack techniques to target businesses; instead of using mass phishing campaigns (as Ryuk and GandCrab have), "an increasing number of attacks are gaining access to a company that has open and exposed remote access points, such as RDP [remote desktop protocol] and virtual network computing," the report stated.

"The concept of ransomware is no longer the concept that we've historically known it as," Raj Samani, chief scientist at McAfee, told SearchSecurity.

Sophos Labs' 2020 Threat Report, which was published earlier this month, presented similar findings. The endpoint security vendor noted that since the SamSam ransomware attacks in 2018, more threat actors have "jumped on the RDP bandwagon" to gain access to corporate networks, not just endpoint devices. In addition, Sophos researchers found more attacks using remote monitoring and management software from vendors such as ConnectWise and Kaseya (ConnectWise's Automate software was recently used in a series of attacks).

John Shier, senior security advisor at Sophos, said certain ransomware operations are demonstrating more sophistication and moving away from relying on "spray and pray" phishing emails. "The majority of the ransomware landscape was just opportunistic attacks," he said.

That's no longer the case, he added. In addition to searching for devices with exposed RDP or weak passwords

**But today's ransomware threats aren't just using more sophisticated techniques to infect organisations – they've also built thriving financial models that resemble the businesses of their cybersecurity counterparts. And they're going after targets that will deliver the biggest return on investment.**

that can be discovered by brute-force attacks, threat actors are also using that access to routinely locate and destroy backups. "The thoroughness of the attacks in those cases are devastating, and therefore they can command higher ransoms and getting higher percentage of payments," Shier said.

Jeremiah Dewey, senior director of managed services and head of incident response at Rapid7, said his company began getting more calls about ransomware attacks with higher ransomware demands. "This year, especially earlier in the year, we saw ransomware authors determine that they could ask for more," he said.

With the volume of ransomware attacks this year, experts expect that trend to continue.

The Ransomware Economy

Samani said the new strategies and approaches used by many threat groups show a "professionalisation" of the ransomware economy. But there are also operational aspects, particularly with the ransomware-as-a-service (RaaS) model, that are exhibiting increased sophistication. With RaaS campaigns such as GandCrab, ransomware authors make their code available to "affiliates" who are then tasked with infecting victims; the authors take a percentage of the ransoms earned by the affiliates.

In the past, Samani said, affiliates were usually less-skilled cybercriminals who relied on traditional phishing or social engineering tactics to spread ransomware. But that has changed, he said. In a series of research posts on Sodinokibi, a RaaS operation that experts believe was developed by GandCrab authors, McAfee observed the emergence of "all-star" affiliates who have gone above and beyond what typical affiliates do.

"Now you're seeing affiliates beginning to recruit individuals that are specialists in RDP stressing or RDP brute-forcing," Samani said. "Threat actors are now hiring specific

individuals based on their specialties to go out and perform the first phase of the attack, which may well be the initial entry vector into an organisation."

And once they achieve access to a target environment, Samani said, the all-stars generally lie low until they achieve an understanding of the network, move laterally and locate and compromise backups in order to maximise the damage.

Sophos Labs' 2020 Threat Report also noted that many ransomware actors are prioritising the types of data that certain drives, files and documents encrypt first. Shier said it's not surprising to see ransomware campaigns increasingly use tactics that rely on human interaction. "What we've seen starting with SamSam is more of a hybrid model – there is some automation, but there's also some humans," he said.

These tactics and strategies have transformed the ransomware business, Samani said, shifting it away from the economies of scale-approach of old. "All stars" affiliates who can not only infect the most victims but also command the biggest ransoms are now reaping the biggest rewards. And the cybercriminals behind these RaaS operations are paying close attention, too.

"The bad guys are actively monitoring, tracking and managing the efficiency of specific affiliates and rewarding them if they are as good as they claim to be," Samani said. "It's absolutely fascinating."

Silver Linings, Dark Portents

There is some good news for enterprises amid the latest ransomware research. For one, Samani said, the more professional ransomware operations were likely forced to adapt because the return on investment for ransomware was decreasing. Efforts from cybersecurity vendors and projects like No More Ransom contributed to victims refusing to pay, either because their data had been decrypted or because they were advised against it.

# Tips For Ransomware Protection On Windows Systems

No one product can prevent every ransomware attack, but there are several defensive practices Windows administrators can take to stop an encryption infection from ruining their day.

By Brian Kirsch, IT Architect and Instructor at Milwaukee Area Technical College

Ransomware. Just the word quickens the pulse of every Windows administrator who might have lingering doubts about the effectiveness of their security approach.

Many IT folks lose sleep over the effectiveness of their ransomware protection setup, and for good reason. Your vital Windows systems keep most companies running, and thoughts of them going offline will have many IT pros staring at the clock at 3 a.m.

Unfortunately, ransomware will hit you in some capacity, despite any measures you take, but it's not a futile effort to shore up your defences. The key is to fortify your systems with layers of security and then to follow best practices for both Windows and your backup products to minimise the damage.

### Give A Closer Look At Your Backup Setup

Backups are something companies make with the hope that they are never needed. Oftentimes, backups are a secondary task that is shuttled to an ops group to be done as a daily task that is a checkbox on some form somewhere. This is how trouble starts.

You need to make backups, but another part of the job is to secure those backups. A backup server or appliance


Photo by freestocks on Unsplash

Looking at the big picture, the Windows firewall gives an additional layer of protection against ransomware. It's already there and should have little performance impact.

is a very tempting target for attackers who want to plant ransomware. These servers or appliances have network access to pretty much everything in your data centre. It's your company's safety net. If this massive repository of data got encrypted, it's likely the company would pay a significant amount to free up those files.

Most backup products are public, which means ransomware creators know how they work, such as how the agents work and their paths. With all that information, an attacker can write software tailored to your vendor's backup product.

Now, most backup offerings have some level of ransomware protection, but you have to enable it. Most people find the setting or steps to protect their data after the backups have been wiped. Don't wait to verify your backup product is secured against ransomware; do it today.

### An Old Security Standby Comes To The Fore

This also brings up a secondary practice: air-gapping. This methodology was popular in the days of tape backup but fell out of favour with the introduction of replication. Some would argue that data that is several weeks or several months old has little value, but is the alternative – no data – any better? Anyone with IT experience who has seen organisations wiped out after a ransomware attack might change your mind if you feel old data is not worth having in an emergency.

A small network-attached storage product you use for a data store dump every six months and lock away suddenly doesn't sound like such a bad idea when the alternative is zero data. It's a relatively inexpensive addition to the data centre used as an extra repository of your data.

Think of it this way: Would you rather get hit with ransomware and lose a few months' worth of data or all 15 years? Neither is a great situation, but one is much preferred over the other. These cold backups won't replace your backup strategy, but rather supplements

Designed by Freepik

it as a relatively economical airgap. When it comes to ransomware, more layers of safeguards should be the rule.

Air-gapping is a practice that is not followed as closely now with the pervasiveness of online deduplication backup products. For organisations that can afford them, these offerings often replicate to online backup appliances in remote locations to make the data accessible.

### Don't Overlook Built-In Ransomware Protection

There are more than a few ways to mitigate the ransomware threat, but using a layered approach is recommended. These malicious applications quickly move east-west across flat networks. Internal firewalls, whether physical or virtual, can do a lot to stop these types of attacks.

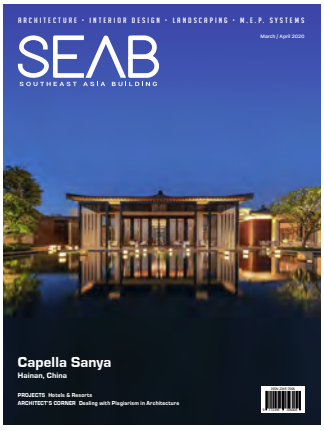
An often-overlooked option is the Windows firewall. When it first came out, the Windows firewall had a few stumbles, but Microsoft continued to develop and improve it to build a solid software firewall. This is a low-cost offering that is free but does require some administration work. The Windows firewall is not going to stop all possible ransomware, but very few products can.

Looking at the big picture, the Windows firewall gives an additional layer of protection against ransomware. It's already there and should have little performance impact.

# 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: _____

*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 | OBC |
| Secutech India 2020 | 7 - 9 May 2020 | Mumbai | India | www.secutechexpo.com | 5 |
| 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/ | 1 |
| IFSEC Philippines 2020 | 22 - 24 July 2020 | Manila | Philippines | www.ifsec.events/philippines/ | 3 |
| GSX 2020 | 21 - 23 Sep 2020 | Atlanta | U.S.A. | www.gsx.org | IFC |
| Safety & Security Asia 2020 | 6 - 8 Oct 2020 | Singapore | Singapore | www.safetysecurityasia.com.sg | 7 |

# 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

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**