MAY / JUNE 2020

SECURITY SOLUTIONS TODAY

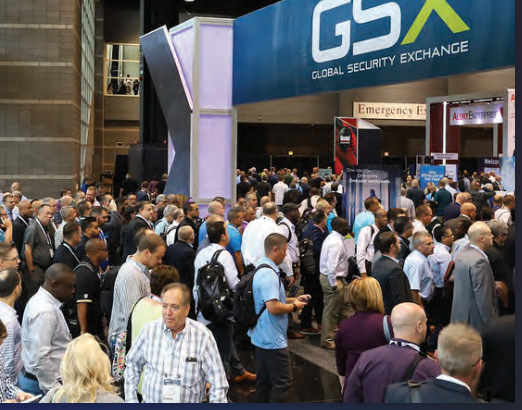
UNRAVELING UNMANNED AERIAL VEHICLES

Regulating the growing applications of drone technology

In Focus
The Evolution Of Data Security Threats

Aviation And Transportation Feature
How Technology Has Reshaped Aviation And Transportation

Biometrics And RFID Feature
RFID Tracking For Asset Protection



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

SHOW RESCHEDULED

NEW DATES

IFSEC SOUTHEAST ASIA

SECURITY FIRE SAFETY

20 - 22 OCTOBER 2020

MALAYSIA INTERNATIONAL TRADE AND EXHIBITION CENTRE (MITEC), KL

SECURITY IS CRITICAL
IFSEC IS ESSENTIAL

ABOUT IFSEC SOUTHEAST ASIA

Widely recognised as the world's leading security, fire and safety portfolio, IFSEC Southeast Asia which is part of ASEAN Super 8 exhibition, will again provide the perfect platform for companies to showcase their latest innovations and activities from 20 - 22 October 2020, at Malaysia International Trade and Exhibition Centre (MITEC), Kuala Lumpur.

With new features, innovative products and technologies, this is a must attend event for all security, fire and safety professionals and it is a crucial exhibition for stakeholders in the industry to bring in and display their products, solutions and technologies.

WWW.IFSECSEA.COM | WWW.SUPER8ASEAN.COM

@IFSECSEA #IFSECSEA | IFSEC Southeast Asia | IFSEC Southeast Asia

WHY IFSEC

- **Connecting** with the security industry
- **Develop Business** with new and existing partners
- **Generate Regional Business** with quality buyers
- **Launch** your latest innovations, products and technologies

Scan to Register

PRE-REGISTRATION IS NOW OPEN!

EXHIBITORS' PROFILE

IFSEC Southeast Asia features exhibitors and products related to the Security, Safety and Fire industries :

- Drones / UAVs
- Emergency Alarm and Warning Systems
- Facilities Management
- Fire Alarms / Detection / Protection
- Fire Prevention and Protection
- Fire Fighting Equipment
- Lighting / Evacuation / Signage
- Occupational, Safety & Health (OSH)
- Perimeter Protection
- Physical Security
- Rescue
- Safe Cities
- Security Consulting
- Security Installation
- Security Management
- Smart Building
- Vehicle / Transport / Fleet / Drivers
- Video Surveillance (CCTV)

VISITORS' PROFILE

IFSEC Southeast Asia welcomes a diverse group of visitors from various industries :

- Banking / Financial Services
- Construction / Developer
- Consultancy
- Cyber Security
- Digital Forensic
- Education
- Government
- Hospital
- Hotels / Clubs
- Importer / Exporter / Distributor
- Installers / Systems Designer
- Insurance
- IT
- Jewelry
- Manufacturers
- Oil & Gas
- Policing / Military
- Property Management
- Publishing
- Retail / Wholesale
- Systems Integrators
- Telecommunications
- Training
- Transportation
- Utilities

CONTACT INFO

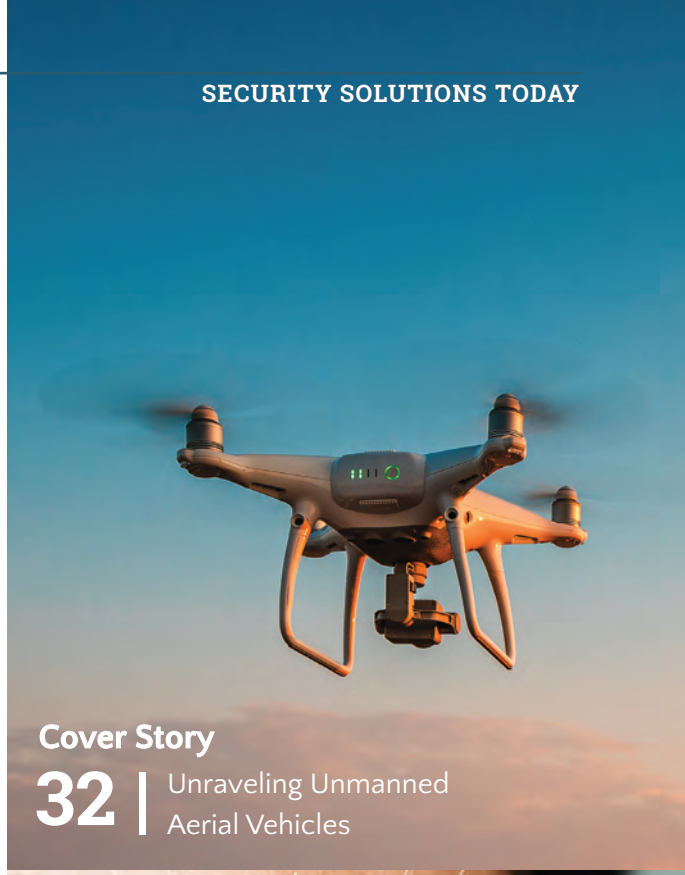
Local & Asia Sales
Hamizan Razali (Mr)
T: +6012 367 1415
E: hamizan.razali@informa.com

International Sales
Shaun White (Mr)
T: +44 207 560 4040
E: Shaun.White@informa.com

Endorsed By: MATRADE

Organised By: informa markets | UBM

IN THIS ISSUE



Cover Story
32 | Unraveling Unmanned Aerial Vehicles

Security Feature
49 | Facial Recognition: Old Myths, New Markets

In Focus
70 | Protect Against Evolving Data Security Threats

IFSEC
PHILIPPINES
SECURITY • FIRE • SAFETY

21 - 23 JULY 2021

SMX CONVENTION CENTER MANILA,
MALL OF ASIA COMPLEX,
PASAY CITY, PHILIPPINES

FACTS AND FIGURES

3500m²
Exhibition Area

Expected **140**
Companies from **20**
Countries and Regions

Expected **200**
Conference Delegates

5 Country and
Region Pavilions

UBM Exhibitions Philippines, Inc.
Unit 1, Mezzanine Floor, Fly Ace Corporate Center,
13 Coral Way, Central Business Park, Pasay City,
Metro Manila, Philippines
T: +632.8551-7718 / 8551-7564
F: +63.2.8839-1306 | E: ifsecph@informa.com

Contact Our IFSEC Philippines Team for More Information

Asia & Local Sales
Rom Peleno (Mr)
E: Romualdo.Peleno@informa.com
M: +63 917 521 4016

International Sales
Shaun White (Mr)
E: Shaun.White@informa.com
M: +44 7976 887088

T: +632 8551 7718 | +632 8551 7564

WWW.IFSECPHILIPPINES.COM

#IFSECPHILIPPINES @IFSECPH

Organized By
informa markets

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)

CIRCULATION
Yvonne Ooi
(yvonne.ooi@tradelinkmedia.com.sg)

Photo & 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

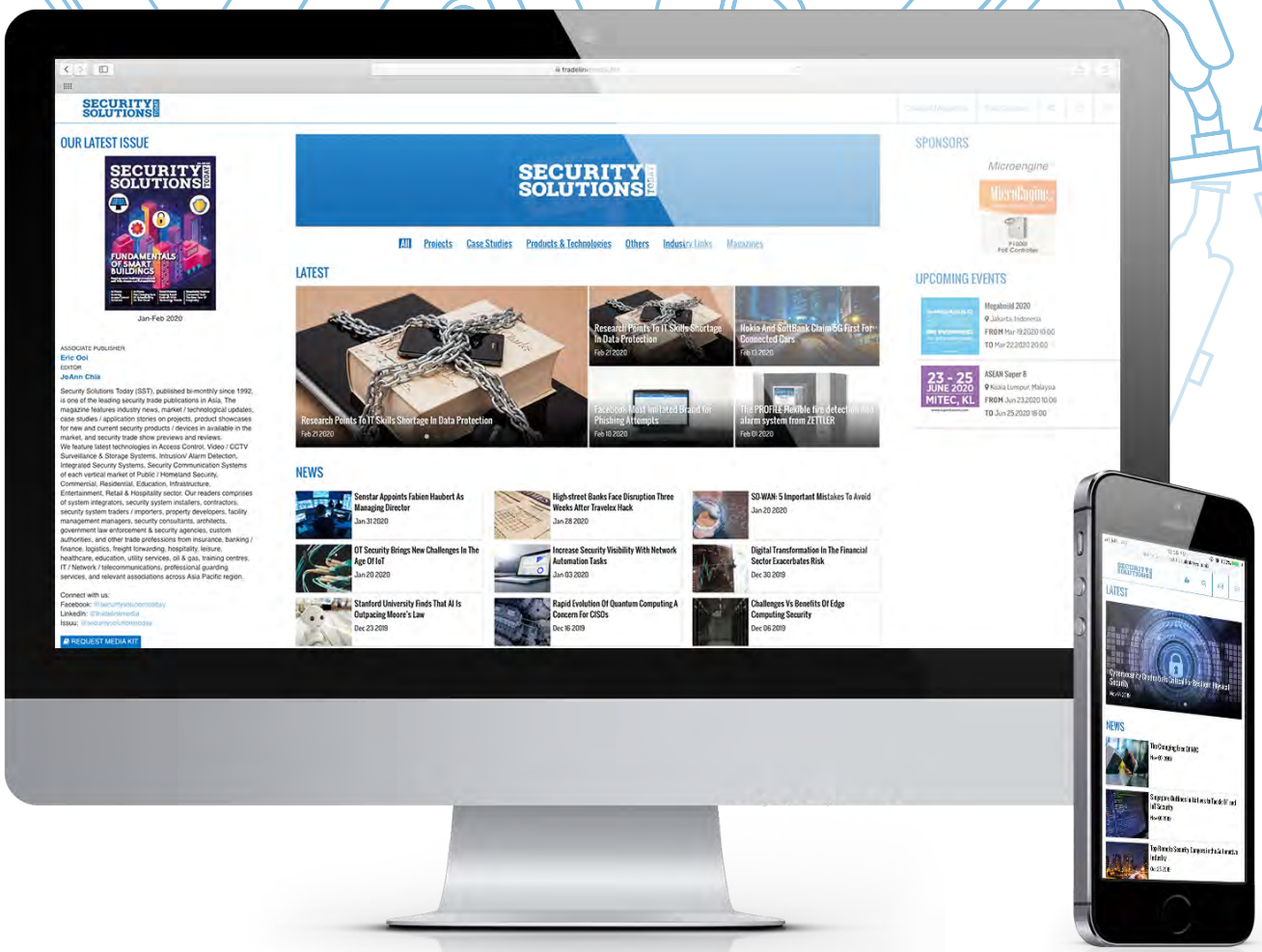
Japan:
T Asoshina/Shizuka Kondo
Echo Japan Corporation
Grande Maison, Rm 303,
2-2, Kudan-Kita,1-chome,
Chiyoda-ku, Tokyo 102,
Japan
Tel: +81-3-32635065
Fax: +81-3-32342064

ISSN 2345-7104
9 772345 710005

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.



sst.tradelinkmedia.biz

Visit our website for the latest information

News on the Industry · Upcoming Exhibitions · Download magazine issues

COMING SOON

JUN 13 – 14 2020

International Conference of Security, Privacy and Trust Management (SPTM)
Helsinki, Finland
– https://csit2020.org/sptm/
sptm@csit2020.org

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 2 – 4 2020

BEX ASIA 2020
Singapore
+65 6780 4594 www.bex-asia.com
info@bex-asia.com

SEP 8 – 10 2020

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

SEP 21 – 23 2020

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

OCT 5 – 6 2020

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

OCT 5 – 8 2020

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

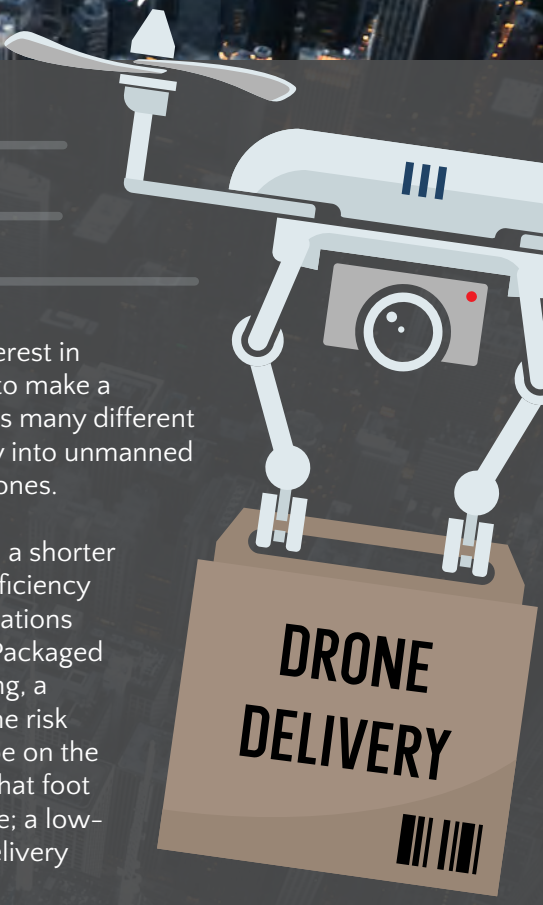
OCT 20 – 22 2020

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

JUL 21 – 23 2021

IFSEC Philippines 2021
Manila, Philippines
+63 2 551 7718 www.ifsec.events/philippines/
www.ifsec.events/philippines/eform/submit/contact

Dear readers,



Along with automation comes a growing interest in unmanned technology, which is expected to make a great impact on efficiency and safety across many different industries. In this issue, we look specifically into unmanned aerial vehicles (UAVs), more commonly known as drones.

From allowing rescue teams to cover more ground in a shorter time as part of disaster response, to increasing the efficiency of urban deliveries, drones have wide-ranging applications depending on the needs of each team and industry. Packaged with other technology like cameras or thermal imaging, a drone can become a powerful tool whilst reducing the risk that its controller would be exposed to should they be on the ground themselves. Drones can also navigate areas that foot or vehicular traffic would be hard-pressed to traverse; a low-flying drone can deliver items more quickly than a delivery van which might be held up by heavy traffic.

For all their strengths, drones too come with their own set of risks and vulnerabilities that need to be tackled to make the technology suitable for widespread use. For one, current regulations are not suitable should the goal be to employ drones commercially on a large scale. There's a fine line to be trod between allowing more flexibility to drone operators, and keeping people safe from the potential misuse of drone technology.

This issue also explores the security advancements in aviation and transportation; with smarter solutions, travel becomes more seamless, and the face of aviation and public transit is changing. We also discuss the changes in Biometrics and RFID technology, and examine the intricacies of privacy and data protection solutions.

2020 has been a rough year, with COVID-19 exposing the healthcare security weaknesses in many countries. The lessons learnt will help to influence and shape future security developments; for now, keep safe while we go about life as best we can in these extraordinary times.

Safe reading!

CJ Chia

Editor

CORONAVIRUS PANDEMIC WILL DRIVE RESPONSIBLE (ESG) INVESTING 'SKYWARDS'

The coronavirus pandemic and its economic fallout will trigger a 'skyward surge' in sustainable, responsible and impactful investing over the next 12 months, affirms the CEO of one of the world's largest independent financial advisory organisations.

The prediction from the boss of deVere Group, which has more than $12bn under advisement, comes as Bloomberg analysis reveals that the average Environmental, Social and Governance (ESG) fund fell by half the decrease registered by the S&P 500 Index over the same period during the Covid-19 crisis.

ESG refers to a class of investing also known as "sustainable investing." The umbrella term covers three main factors. 'E' is for 'environment' and includes issues such as climate change policies, carbon footprint, and use of renewable energies. 'S' is for 'social' and includes workers' rights and protections. 'G' is for 'governance' and includes diversity of the board and corporate transparency.

Mr Green comments: "The coronavirus pandemic will trigger a 'skyward surge' in sustainable, responsible and impactful investing over the next 12 months for three key reasons.

"First, before the pandemic, research has revealed that investments that score well in terms of ESG credentials often outperform the market and have lower volatility over the long-run.

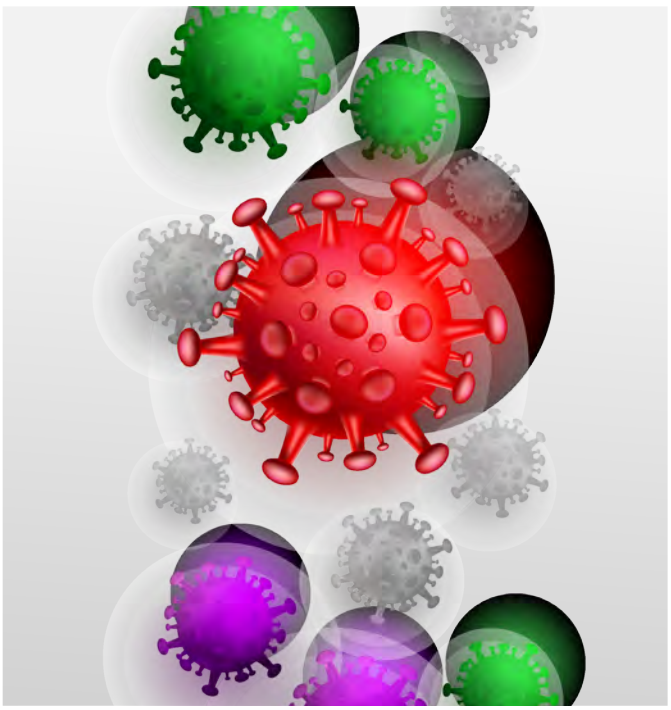
"Since the Covid-19 public health emergency up-ended the world, the latest broad analysis shows that ESG funds have typically continued to outperform others."

He continues: "Second, the coronavirus pandemic has underscored the vulnerability and fragility of societies and the planet.

"It has underscored that increasingly companies will only survive and thrive if they operate with a nod from the wider court of public approval.

"It has underscored the complexity and interconnectedness of our world in terms of demand and supply, in trade and commerce – and how these can be under threat if not sustainable."

Mr Green goes on to add: "Third, demographic shifts will support the trend. Millennials - those who were born in the time period ranging from the early 1980s to the mid-1990s and early 2000s – cite ESG investing as their top priority when considering investment opportunities.



"This is crucial because the biggest-ever generational transfer of wealth – likely to be around $30trn - from baby boomers to millennials will take place in the next few years."

In January, deVere Group carried out a global survey that revealed 77% of millennials said that Environmental, Social and Governance (ESG) investing was their top priority when considering investment opportunities.

This survey highlighted that whilst traditional factors – such as anticipated returns (10%), past performance (7%), risk tolerance (4%) and tactical allocation (2%) – are important factors in millennial respondents' investment decision-making, they are no longer enough by themselves.

Nigel Green concludes: "ESG investing was already going to reshape the investment landscape in this new decade – but the coronavirus will quicken the pace of this reshaping.

"Investors are increasingly aware that it is possible - and increasingly necessary - to make a profit while positively and proactively protecting people and the planet.

"As such, they will be making investment decisions after measuring the sustainability and societal impact of a sector or company as these criteria help to better determine their future financial performance, or in other words their risk and return." ■

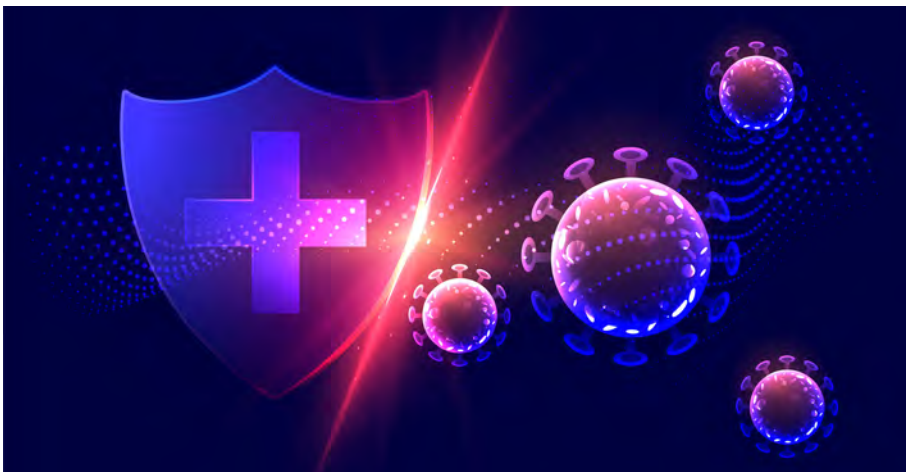
LORCA CALLS ON SECURITY SCALEUPS TO TACKLE CORONAVIRUS CHALLENGE

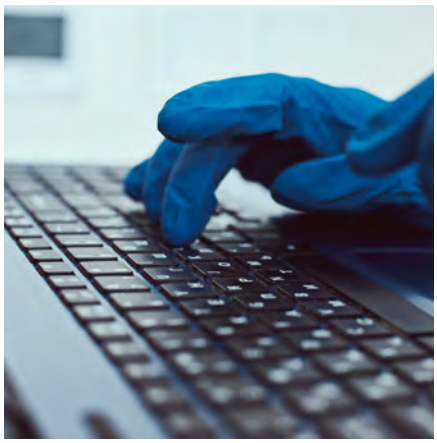
The London Office for Rapid Cyber Security Advancement (Lorca) is on the hunt for security scaleups to address the challenges thrown up by the Covid-19 coronavirus pandemic, such as securing remote workforces and digital citizen services, and tackling disinformation.

As with previous groups, the fifth cohort of scaleups to move through Lorca's scheme will receive support in scaling their businesses, securing investment, accessing new markets, and expanding internationally. The ultimate aim is to grow the UK's cybersecurity industry and help make the internet a safer place to be for all.

As usual, the selected scaleups will receive mentoring, access to networking opportunities with investors, and commercial and engineering expertise from Lorca's delivery partners, including consultancy Deloitte and Queen's University Belfast's Centre for Secure Information Technologies (CSIT), and corporate partners including Lloyds Banking Group, Dell, Kx, Kudelski Security and the Global Cyber Alliance.

"As well as meeting the needs of industry today, Lorca catalyses innovation that caters to the cybersecurity challenges on the horizon that will intersect both society and business and require new models of collaboration to solve," said Saj Huq, Lorca programme director.





"We know there is cutting-edge technology available to meet these challenges, and we want to ensure those solutions get the support they need to scale, access the right funding and develop in direct response to what the market requires.

"Coupled with this, the current global pandemic has underlined and increased our reliance on technology. With this, it has brought very real cybersecurity challenges to the fore. This is a time to support the cybersecurity innovations that our digital world needs most and we look forward to enabling this next wave of high-potential SMEs to scale and succeed."

"At this time of Covid-19 related international emergency we are seeing the online spread of disinformation aggravate the public health crisis, rapid adoption of remote working putting pressure on information security and malicious actors seeking to take advantage of weak links in cybersecurity and overburdened IT teams," said Louise Cushnahan, head of innovation at CSIT.

"Sometimes the most innovative, resilient and successful companies grow out of times of uncertainty and adversity. Our highly experienced academic and engineering teams are looking forward to engaging with and delivering impactful support for Cohort Five in the months ahead," she said.

Huq said that, over the years, the industry has made it clear to Lorca that it needs "new breeds" of security products and services to tackle the growing complexity of the digital world, so it is particularly keen to support innovators working on what it sees as the next frontier for security, with solutions that protect individuals across the full spectrum of their digital lives – something that has become highly relevant over the past fortnight.

This includes, for example, securing digital workforces; fighting back against disinformation, fake news and social media trolls; and enhancing user privacy. Lorca said that as data becomes a kind of digital currency, the tech sector must adapt to serve individual needs, and not those of corporations, building trust in technology and empowering normal people to take back control of their digital lives. ■

NHS ROLLS OUT VIDEO CONSULTATIONS AT GPS TO SUPPORT LOCKDOWN

The digital unit of the health service NHSX is working with NHS England and NHS Improvement in a deployment of video consultation systems in GP practices across the country.

The technology is seen as essential to reduce face-to-face contact to protect patients and staff, minimise the risk of Covid-19 infection and care for people who are not infected but are mostly staying at home.

According to Diane Baynham, NHSX's head of service design digital urgent and emergency care, and Mary Hudson, deputy director for digital first primary care, many practices already have these tools and usage has increased rapidly in recent weeks.

However, many GPs who have the service available have not yet begun to use it. EMIS is one of the biggest GP IT system providers in England, with nearly 4,000 GP practices using its EMIS Web service. In 2017, it launched its Video Consult service, but uptake has been limited.

This echoes throughout GP practices in the UK – suppliers often offer the service, but few GP practices use it. EMIS, which normally charges GPs for the use of video consultations, has now decided to offer it for free for the next few months.

According to NHSX, practices that still don't have technology to consult remotely will be allowed to use video conferencing tools such as Skype, WhatsApp and Facetime as a short-term measure, it said in a blog post.

However, the NHSX staff noted that the ideal scenario is to only use video products that the Digital Care Services Framework (DCS, also known as GPIT Futures) can be confident that are appropriate and secure.

NHS Digital has fast-tracked assurance video consultation products that will be centrally funded, and a list of approved suppliers that can be immediately called off by commissioners was made available from 25 March 2020. ■

UPTIME INSTITUTE ADVISES OPERATORS TO SUSPEND NON-ESSENTIAL DATACENTRE PROJECTS

Datacentre operators are being urged to consider postponing or cancelling any upgrades or migration projects to reduce the risk of their IT staff contracting the Covid-19 coronavirus.

An 18-page advisory document published by the Uptime Institute datacentre resiliency think-tank sets out the steps that datacentre operators of all types – from multi-tenant colocation facilities to private datacentres and server farms housed within mixed-use facilities – should take to protect their staff during the pandemic.

This includes "avoiding unnecessary risks", such as embarking on projects that put staff at heightened risk of infection, and put additional strain on suppliers.

Also, given the economic impact coronavirus is having on businesses across the world, the document said it might be prudent for some companies to press pause on such projects to reduce their risk of "cash flow" exposure, too.

"For organisations involved in datacentre construction, major upgrades or extensions of capacity, the pandemic presents challenges," says the document.

"Construction speed has a big impact on cost, and delays in one area can impact many other areas and other suppliers. In this case, however, delays may be advisable."

To be continued on page 11

The document says all all non-essential projects should be suspended "when possible", but if work must continue, the Uptime Institute recommends introducing safeguards to ensure project team members are kept away from those providing operational, day-to-day support for sites.

"If possible, create a separate, secure entrance for all parties involved in the project and establish isolation of the project personnel from the operations personnel," says the document.

"Operations team members who are assigned to project oversight or supervision should be dedicated to those duties and not allowed to interact with duty operations personnel."

The document also makes the case for operators to postpone all "non-essential" maintenance tasks and reschedule high-risk testing until after the pandemic subsides, and to prepare for component shortages and supply chain disruption.

"Anticipate and prepare for supply-chain disruptions on items such as cabling, server racks, critical infrastructure spares and other components," it says. "Order more inventory and discuss projected lead times with vendors and suppliers.

"Develop plans to deal with the possibility of a major equipment failure when you may not have access to key personnel or resources owing to supply-chain disruptions."

The datacentre sector is at heightened risk of disruption as a result of the coronavirus, the document warns, because of severe skills shortages in certain geographies, which make it extremely difficult to find replacement staff with the right knowledge and expertise to plug any gaps.

"Current events reinforce the need for increased efforts on the part of the industry, educational institutions and trade organisations to strengthen recruitment and training programmes," says the document.

"Similarly, the use of automation and remote monitoring can enable facilities to operate more effectively, and for longer, with less need for on-site staff. The pandemic may accelerate the long-term trend in this direction."

In the interests of safeguarding the health and wellbeing of the staff that datacentres do have, the document makes a series of recommendations about the steps that should be followed by operators during the pandemic.

It includes practical advice on ensuring staff have access to hand sanitiser and disinfecting wipes throughout the facility, and to conduct multiple cleaning rounds each day, taking in heavy-contact surfaces such as door handles, light switches and hand rails.

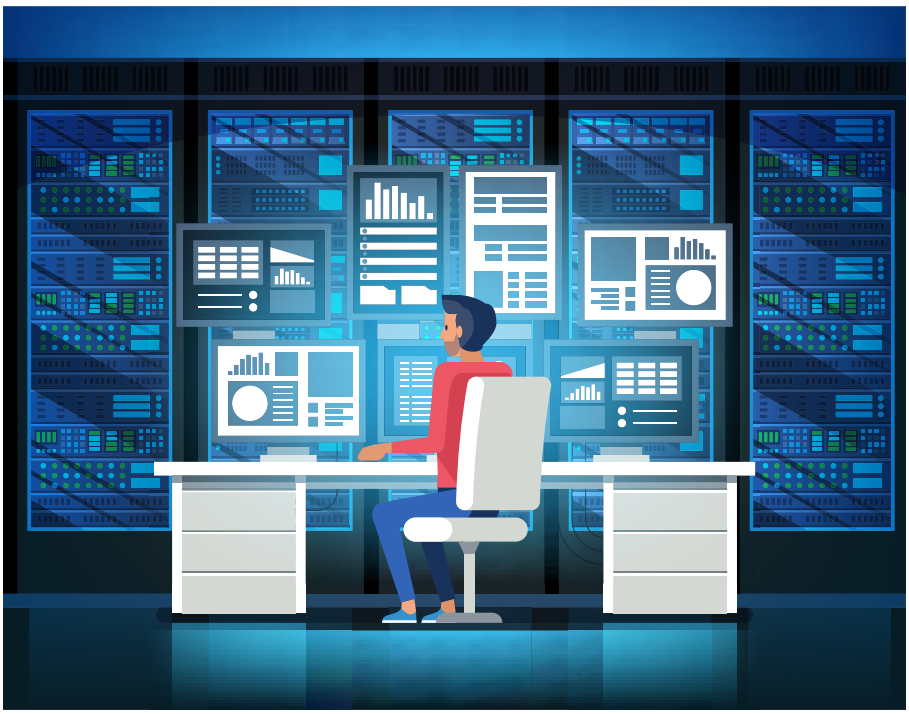
It also suggests that operators suspend the use of "mantraps" at the entrances of their data halls, which are traditionally used to reduce the risk of authorised datacentre personnel being "tail-gated" into data halls by people who do not have the necessary access credentials.

However, the report says the use of mantraps could act as a "repository" for the virus because they are typically small, confined spaces without ventilation.

"Consider limiting the use of them and/or sanitising them after each use," says the Uptime Institute advisory.

The document also makes the point that datacentres are treated by operators as mission-critical facilities, and that "preparedness" is in "the industry's DNA", which makes it more than capable of rising to the coronavirus challenge.

"Thanks to their focus on performance, efficiency and reliability – tested through prior experience with power blackouts, wildfire, adverse weather and other potentially disruptive events – most datacentre owner/operators have contingency plans in place that can be adapted to the challenges of the current pandemic," it adds. ■



PING IDENTITY ANNOUNCES NEW WORKFORCE AND CUSTOMER AUTHENTICATION

Ping Identity, the Intelligent Identity solution for the enterprise, have announced two new solution packages for enabling centralised authentication services, which span the entire enterprise.

The new solutions include single sign-on (SSO), multi-factor authentication (MFA), user directory, and complementary Ping Professional Services that enable extraordinary customer and workforce digital experiences.

These new solutions, Customer360 and Workforce360, are designed to address the full range of enterprise needs including hybrid IT integration, advanced configuration, and are now available with simple pricing and are deployable with flexible cloud options.

Ping's new solution for customer identity, Customer360, ensures seamless customer experiences during registration, login, multi-factor authentication, and self-service profile management to help you attract and retain customers.

A modern customer identity management solution provides a seamless front door to today's digital businesses, improving conversion rates and retention across digital customer journeys. Ping's Customer360 provides consistent login experiences and secure passwordless authentication options for an organisation's digital properties, helping increase user engagement and increase sales.

Ping's Customer360 also includes MFA capabilities that can be tailored to diverse security requirements and customer preferences. These capabilities range from widely adopted SMS or email options for MFA, to the ability to verify customer identities and transaction approvals with fingerprints or face scans from a mobile app.

Ping's new solution for workforce identity, Workforce360, provides secure, consistent authentication experiences to employees no matter where work gets done. It includes a centralised authentication solution with MFA and directory that creates a modern identity foundation to make large enterprises more productive, secure, and agile.

Ping's Workforce360 provides an identity solution that is capable of extending across diverse hybrid IT environments with speed, scale, and security.

It provides fast, out-of-the-box integrations and the ability to easily extend across SaaS, legacy applications, cloud applications and more for seamless login experiences, helping increase security and employee productivity.

Both Customer360 and Workforce360 leverage the latest cloud technologies including cloud-ready software, Identity-as-a-Service capabilities, and complementary Ping Professional Services for a comprehensive solution package.

Both solutions stand apart in the market with their breadth of integration, extensibility, and configuration options valued by enterprises, as well as the flexibility to:

- Deploy in almost any cloud environment
- Authenticate users for practically any application, any directory, and any situation
- Package with complementary Ping Professional Services to accelerate time-to-value
- Simplify pricing with no add-on costs for expected features

Loren Russon, vice president of product management, Ping Identity, said: "With the ability to deploy quickly in any cloud—whether it be public, private, or a hybrid environment—our new solutions will help global enterprises efficiently tackle and simplify some of their most complex security and user productivity challenges, while enabling line of business initiatives and supporting corporate IT teams with advanced use cases.

"With a focus on the workforce and customer identity experiences, companies will be able to swiftly implement these market leading capabilities throughout their organisations to accelerate digital transformation objectives." ■

CORONAVIRUS LOCKDOWN: MASSIVE SURGE IN THE USE OF FINTECH APPS

Coronavirus-triggered social distancing, isolation and lockdowns have driven-up the use of financial apps in Europe by 72 per cent in a week, reveals deVere Group, one of the world's largest independent financial advisory organisations. The sharp increase in the use of financial technology comes as the world readjusts to life fighting against the global health crisis and economic downturn caused by the Covid-19 pandemic.

James Green, deVere Group's Divisional Manager of Europe, notes: "The world has changed in the last few weeks. The measures we're now all taking to help the fight back against coronavirus are affecting the way we interact, live, work, and take care of our finances.

"A new era has already begun, with digitalisation and new technologies driving the shift. This can be seen by demand soaring for video-calling platforms such as Google Hangouts, Skype, FaceTime and Zoom amongst others, as more people from ever work remotely.

"Indeed, Zoom Video Communications has been a remarkable performer in recent times, with its shares gaining more 32% since the market began its decline in mid-February."

"This new era has also been evidenced this week with a staggering 72 per cent jump in the use of our fintech [financial technology] apps from existing clients and a sharp increase in enquiries from potential ones."

He continues: "Since the 2008-2009 financial crash, fintech has been filling the void left between what traditional financial services companies are offering and what clients are now expecting, especially in terms of customer experience.

"In broad terms, this means immediate, on-the-go, 24/7 access to, use and management of their money. It means personalised, on-demand services. It means lower costs.

"It can be expected that due to the Coronavirus pandemic and the steps being taken to combat it, this move towards fintech will be significantly accelerated. "Fintech is fast-becoming the new normal."

deVere is one of the very few financial advisory organisations that has been actively pushing into fintech and is now widely regarded as one of the leaders in the sector. Over the last three years, the company has developed and rolled out a suite of ground-breaking fintech apps. These include deVere Vault, a global e-money currency app and multi-currency prepaid card; deVere Crypto, a

cryptocurrency app to store, transfer and exchange major cryptocurrencies, including Bitcoin; deVere Core, an app that allows clients to monitor their investments in real-time on-the-go, keeping them informed with news and events that impact investor returns; and deVere Catalyst, a low-cost investment and savings app that offers best-in-class globally diversified funds.

James Green observes: "deVere Catalyst, in particular, has seen a surge in usage over the last week. This app takes the hassle out of investing and gives those with little or no investment experience the opportunity to invest in well-balanced funds at a fraction of the price – thereby helping them to reach their life-enhancing long-term financial goals."

Against the backdrop of Covid-19, last week, deVere Group, which operates in more than 100 countries worldwide, launched its Contactless Advice service.

At the launch deVere Group CEO and founder Nigel Green said: "Experts agree that very seldom is it a good idea to take a DIY-approach to something so fundamental to your life as your finances. With the financial and economic landscape shifting and evolving so rapidly, this, I suggest, is certainly not the time.

"With this free service that offers professional, independent advice, there's no need to do that."

deVere's Divisional Manager of Europe concludes: "Fintech – a significant driver of the so-called 'fourth industrial revolution' – is going to become an increasingly dominant part of our lives and coronavirus is fuelling the shift.

"I believe it'll have a positive impact. Why? Because it is meeting evident and growing client demand for on-the-go service, it is speeding up the advance of financial inclusion across the world, plus it gives firms the opportunity to diversify, cut costs, meet regulatory requirements and further enhance the client experience." ■

RESEARCH SHOWS COMPANIES EMBRACING CLOUD-BASED SECURITY TOOLS, BUT CONCERNS REMAIN

Exabeam, the Smarter SIEM™ company, today announced the results of a security practitioner survey that revealed while many companies are beginning to migrate security tools to the cloud, a significant number have concerns. The survey, conducted at the Cloud and Security Expo in London, highlights data privacy, unauthorised access, server outages and integration as key concerns.

The survey shows a mixed picture when it comes to firms migrating security tools to the cloud. While just over half of respondents (52 percent) began migrating to cloud-based security products during or before 2018, around a fifth (18 percent) waited until 2019, three percent started in 2020, 13 percent have not yet started and the remainder don't know when they'll migrate.

Of those that have started their migration, over half (58 percent) have migrated at least one quarter of their security tools to the cloud, while one third (33 percent) said more than 50 percent of their security tools are now cloud-based.

Typically, organisations migrate security tools to the cloud to minimise the resources and overhead associated with owning and maintaining on-premises equipment and software. This means security teams can avoid system sizing, maintenance, uptime management, and product upgrades. Reducing engineering effort to deploy and maintain new solutions allows security analysts to complete tasks faster and frees engineers up to focus on other projects.

The survey results support this, with improvements in monitoring and tracking of attacks (29 percent) and reduced maintenance (22 percent) considered the most important gains from using cloud-based security tools. CAPEX reductions (18 percent), faster time to value (17 percent) and access to the latest features (13 percent) are drivers for cloud adoption, but considered less important.

However, when asked what concerns they have about moving security tools to the cloud, data privacy (30 percent) remains high on the list, with unauthorised access (16 percent), server outages (14 percent), integration with other security tools (14 percent), and data sovereignty (13 percent) also being raised.

While 22 percent stated migration to the cloud was not a priority for their organisation, the results suggest a lack of understanding about the migration issue as a whole. Around a third (32 percent) said they did not know what concerns their organisation has about moving security tools to the cloud.

Furthermore, despite about a third (32 percent) of respondents saying they consider it to be too difficult or too risky to migrate security tools to the cloud, nearly half said their preference is to migrate legacy products to the cloud (46 percent) rather than replace legacy on-premise products with new cloud-native security tools (54 percent).

Organisations are protecting a variety of data types with cloud-based security tools, with email the most widely protected (22 percent), followed by customer information (21 percent), file-sharing (20 percent) and personnel files (18 percent). However, few organisations (12%) have extended cloud-based security to protecting corporate financial information.

"As organisations modernise their security operations, SaaS solutions are increasingly becoming the deployment model of choice. While the results of this survey show that some security professionals still have concerns, having visibility into cloud services is vital and many organisations are now taking a cloud-first approach to security," commented Sam Humphries, security strategist, Exabeam.

"We can expect more organisations to migrate their security tools to the cloud this year as security professionals increasingly see the benefits of hosted cloud offerings, which provide the full functionality of traditional on-premise solutions. Added benefits include reduced cost and maintenance issues, as well as eliminating the need to route cloud data to on-premises data centres," concluded Humphries. ■

NETFLIX DOWNSCALES CONTENT RESOLUTION TO EASE STRAIN ON EU NETWORKS

Despite the guarantees of European operators that their networks could cope with the added strain of millions of more people working from home as a result of the coronavirus outbreak, it would appear that politicians are beginning to worry about overuse as leading global video-on-demand service Netflix has acceded to European Commission requests to downgrade the quality of its output.

Thierry Breton, European commissioner for internal markets, revealed that he has been in contact with Netflix CEO Reed Hastings to appeal for the video-on-demand service to end broadcasting content in high definition (HD) and switch to the substantially less network-intensive standard definition (SD).

In a tweet explaining the purpose of his actions, commissioner Breton said: "Teleworking and streaming help a lot but infrastructures might be in a strain. To secure internet access for all, let's #SwitchToStandard definition internet when HD is not necessary."

The continent's operators have been divided as to what the effect on networks the added millions would have.

In Spain, in an unprecedented joint statement, the nation's leading operators – Movistar, Orange, Vodafone, Grupo Masmovil and Grupo Euskaltel – revealed that both fixed and mobile telecommunications networks had experienced a traffic explosion in recent days as a result of the spread of coronavirus and the resulting measures and recommendations sending people home.

Even though they noted that the country was a European leader in terms of fibre optic infrastructure and had one of the best mobile networks in Europe, the Spanish operators appealed that rational and responsible use of the networks would allow all stakeholders – such as service providers, companies and individuals – to ensure that the nation has a quality communication ecosystem that was sustainable over time, in the face of a scenario of increased work and remote schooling that may last several weeks.

In the UK, the country's leading public network providers BT and Virgin Media have both expressed confidence. The UK's second largest broadband provider, Virgin Media, stressed that as more people may be working from home at the moment, it was important for users to know that its network could withstand any increased usage, including peaks throughout the day, in the evenings and at weekends.

Virgin assured that as usage inevitably rose, its existing capacity would be able to take the strain, and that it was monitoring closely on network issues and was ready to make changes if needed. For its part, BT added in a video on 13 March that its network peaks for traffic in the evening between 8.00pm and 9.00pm when network capacity reaches about 17Tbps (terabits per second). This, it said, was mainly driven by people streaming or downloading the latest software and latest updates for online and console games, adding that the peak is around 10 times what it saw from households over the day.

In all, BT was confident that it could accommodate people working from home, and their work-from-home traffic, on both its core and access networks provided by its Openreach division.

In what may be a cultural difference between the US and Europe, leading comms provider Verizon released data on 18 March showing that it was games rather than streaming video that had shown the greatest increase on its networks. The provider said that while video such as Netflix has seen a 12% week-on-week increase, gaming had spiked by 75%. Meanwhile, VPN usage had shot up 34%. ■

PERPETUITYARC TRAINING RESPONDS TO SURGE IN DEMAND FOR ONLINE LEARNING COURSES

PerpetuityARC Training, part of Linx International Group – the world's leading provider of accredited security systems training courses – is responding to a surge in demand, for its portfolio of online training courses. The company is experiencing unprecedented international demand from organisations of all sizes, operating across a wide range of sectors, as they look to ensure they have the skills in-house to coordinate their response to the rapidly changing coronavirus situation.

Director of Sales and Marketing at the Linx International Group, Sarah Hayward-Turton states: "Even the most well-prepared organisations with extensive contingency plans, based on thorough risk assessments, have been stunned by the scale and speed of the situation we currently face." She adds: "Key personnel off sick or isolated, travel restrictions, offices and stores shutdown, supply-chain issues affected by manufacturing shortfalls, import delays, and panic-buying. These are just some of the issues impacting organisations right now. The scale is unprecedented, but effective risk, crisis and disaster management begins with preparation for the worst-case scenario."

Hayward-Turton adds: "We are helping small businesses with no continuity strategy, through to large multi-national organisations who want to train more employees on the latest methodologies and best practice, to ensure that expertise resides in-house, to help manage their response to this crisis, as well as being as ready as possible for what the future may bring."

Crucially, the accredited training courses provided by PerpetuityARC Training are available online and all offer CPD points. Courses range from bite-sized introductions, through to formal accredited security risk management programmes.

Online training courses available today include:

▪ **Security Risk Management** – Learn how to identify threats, risks and vulnerabilities, and create a comprehensive plan that will enable practical measures to be applied to mitigate the impact.

▪ **Crisis Management & Business Continuity** – Learn about risk assessments, how to identify threats, and how to build a crisis management team

▪ **Risk, Crisis and Disaster Management** – BTEC Level 4 qualification of immediate benefit to those working as security managers, intended to introduce and develop security and risk management to the highest level. The syllabus includes: risk communications, business impact analysis, continuity planning and crisis management, forming and operating a crisis management team, command and control structure and liaison with the emergency services.

▪ **Managing Security Risk in the Oil and Gas Sector** – IQ Level 4 qualification addressing some of the more complex risks associated with the oil and gas industry in a range of environments and examines the risks in upstream and downstream operations. Topics covered include: security risk analysis, corporate social responsibility, human rights, and community management, managing activism risk, managing acts of militancy and terrorism against the oil and gas sector, oilfield and pipeline security, refinery security, maritime and offshore security and downstream (retail security).

Hayward-Turton concludes: "Whilst there is no precedent in modern times for the global situation we are facing, there are tried and tested tools, techniques and methodologies that every organisation can put in place today that will help." ■

PRIVATE SECTOR GROUP AIMS TO BUILD PANDEMIC RESILIENCE USING DATA VISUALISATION

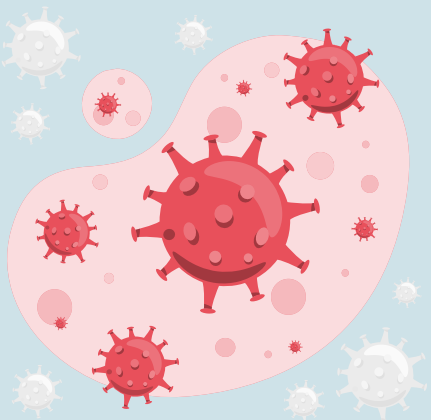
Qlik.org, the philanthropic wing of the Sweden-based data visualisation supplier, has been working as part of a collaborative private sector effort to better analyse epidemic information.

The group, called the Private Sector Roundtable, involves GE, AstraZeneca, Johnson & Johnson and Merck, as well as Qlik. It was set up by Alan Tennenberg, of Johnson & Johnson, and David Barash, of the GE Foundation, following the Ebola crisis in West Africa from 2014-16.

Julie Kae, executive director and global head of corporate responsibility at Qlik.org, says the role of the PSRT is to provide a collective organisation for NGOs – such as the World Health Organisation (WHO) and the US Centers for Disease Control and Prevention (CDC) – to engage with.

It supports the goals of the "Global Health Security Agenda", which is a group of 15 countries, international organisations, and NGOs, as well as private sector companies.

Its chairman, Roland Driece, says on the GHSA website: "When the international community comes through this [Covid-19] outbreak, GHSA will lead partnerships to incorporate lessons and implement new resilience measures.



"Because disease is a natural part of our world, it's not a question of if but when the next outbreak will be," he says.

Kae gave as an example of the software donation that Qlik has done through the PSRT, an app they built to render the data locked in WHO PDFs more analysable. These PDFs are lengthy reports on how countries are positioned with respect to health security, and they embody months of work by 30-40 people. With respect to coronavirus, this sort of work will help with resilience for the future, she says. Live data science on the virus and its spread is more the provenance of the likes of the John Hopkins University of Medicine in the US and, in the UK, the experts feeding into the Scientific Advisory Group for Emergencies, including the Imperial College, London Covid-19 Response Team.

Kae says Qlik's "ability to blend data from disparate sources in associative models is useful for these type of problems" where data scientists are using machine learning on data sets – epidemiological, in the case of Ebola and Covid-19. But the work of the PSRT is more about strengthening health systems in the most vulnerable areas around the planet ahead of the next outbreak.

Qlik.org is also working with other NGOs, such as the charity Direct Relief which will combine supply chain data with Coronavirus data in a dashboard to help it prioritise where Covid-19 items, such as gloves, masks, gowns, and other protective equipment should be sent. ■

NORWEGIAN CRUISE LINE SUFFERS DATA BREACH

A major cruise operator has suffered a data breach as the travel industry battles the storm created by the COVID-19 outbreak.

Information from a database belonging to Norwegian Cruise Line was discovered on the dark web by an intelligence team at DynaRisk on March 13.

Data exposed in the incident included clear text passwords and email addresses used to log in to the Norwegian Cruise Line travel agent portal by agents working for companies including Virgin Holidays and TUI.

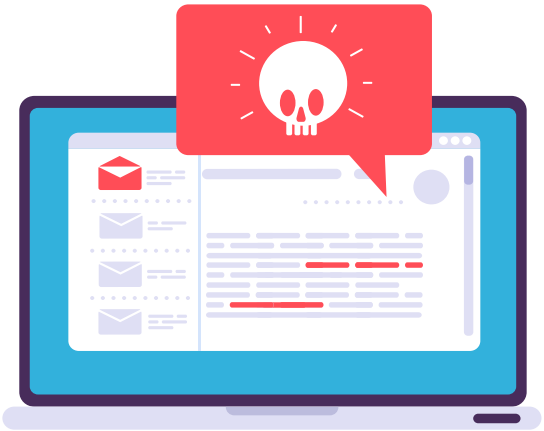
DynaRisk said data relating to 29,969 travel agents was breached from the portal on the agents.ncl.eu website on March 12.

"After verifying that the data records are legitimate credentials, we notified a Norwegian Cruise Line representative immediately. Despite opening our message later that day, we received no response. After five days a representative responded to our team to discuss the breach," said a DynaRisk spokesperson.

DynaRisk said that the incident left agents who were "already vulnerable at this time" at higher risk of cybercrime.

A DynaRisk spokesperson said: "They are now exposed to account takeovers on numerous platforms, sophisticated phishing emails and fraud, which could put further pressure on large travel agents or worse still, put smaller agents out of business."

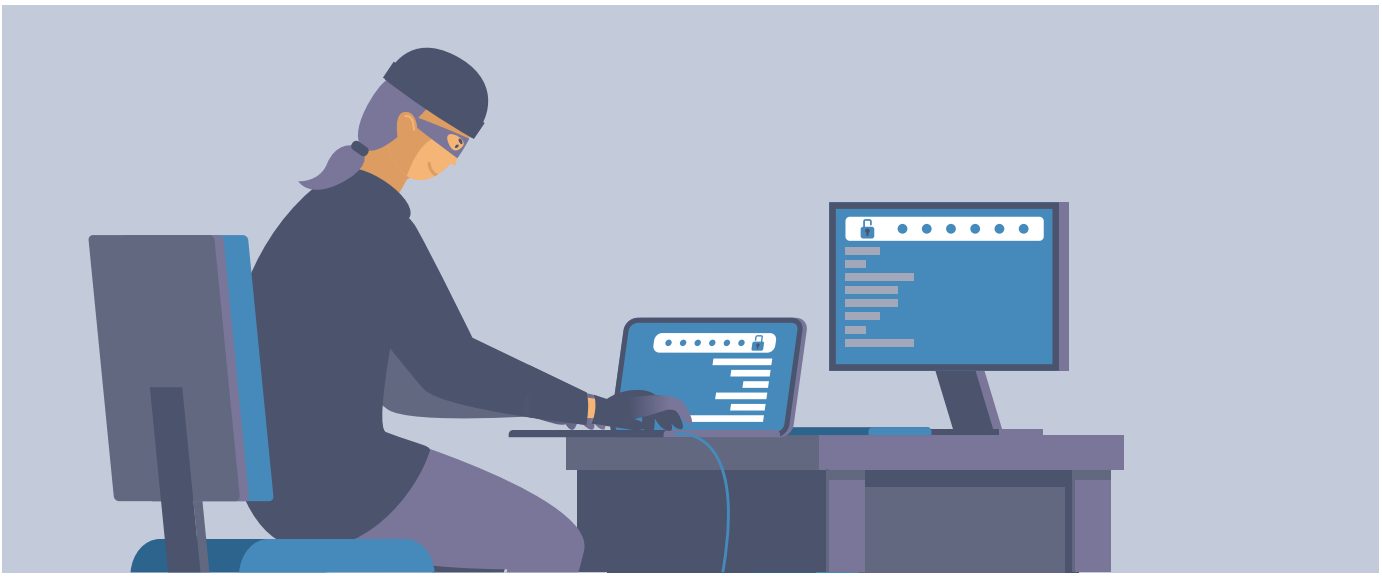
Norwegian Cruise Lines told Infosecurity Magazine: “It has recently come to our attention that the agents.ncl.eu



website may have been compromised. In an abundance of caution, we are in the process of asking certain travel partners that may have been affected to change their password for the site and any site for which they may have used the same password, and to remain vigilant of any suspicious activity or emails.

"We believe limited personal information was involved, specifically names of travel agencies and business contact information such as business addresses and email. This appears to be a unique and isolated incident that involved only a regional travel partner portal which houses marketing materials and educational information and did not involve guest data. We are deeply committed to protecting the security and confidentiality of information and regret any concern this matter may have caused."

Norwegian is the third cruise line this month to hit the cybersecurity headlines. Princess Cruises and Holland America Line both reported being hacked on March 2. ■



UK MAKES ITS CASE FOR POST-BREXIT DATA ADEQUACY DECISION

The UK government has set out its stall in preparation for a series of upcoming assessments by the European Commission (EC) as it seeks to secure adequacy decisions from Brussels to maintain the free flow of personal data after the Brexit transition period ends.

In a series of newly published documents, the government emphasised the UK's "world-class" data protection regime and stressed the contribution the UK made to the development of the European Union (EU) General Data Protection Regulation (GDPR).

"The continued free flow of personal data is vital for the future relationship between the UK and the EU," said the government in its preamble. "Imports and exports of both goods and services heavily depend on the free flow of personal data between the UK and the EU.

"EU personal data-enabled services exports to the UK were worth approximately £42bn (€47bn) in 2018, and exports from the UK to the EU were worth £85bn (€96bn).

"Given these economic ties and our shared commitment to high data protection standards, the government believes it is in both parties' interests to act quickly to ensure the reciprocal free flow of personal data between the EU and the UK.

"The UK government stands ready to assist the Commission in undertaking an assessment to allow the adoption of adequacy decisions for the UK and Gibraltar. We have made arrangements to allow for the free flow of UK personal data to the EU."

Adequacy decisions are a legal mechanism by which the EC facilitates personal data transfers from the EU to third countries – they can encompass data flows under Article 45 of the GDPR for general and commercial purposes, as well as data flows under Article 36 of the Law Enforcement Directive (LED) for law enforcement needs.

A decision in the UK's favour will, in effect, confirm that the country's data protection standards are "essentially equivalent" to those of the EU and are adopted based on a "positive assessment of the third country's data protection framework by the EC".

The UK is taking the position that because the 2018 Data Protection Act and the GDPR were developed hand-in-hand with the EC, they provide comprehensive protections for data subjects that are already equivalent to those in EU law.

The UK's protections include principles to protect personal data in terms of lawfulness, fairness, transparency, purpose

limitation, data limitation, accuracy, storage limitation, integrity and accountability; clear grounds limiting when processing of personal data is lawful; effective and enforceable rights that give individual citizens control over their data in terms of requesting access, information on how it is being used, corrections to it, and deletion; limits and conditions to make sure that when restrictions to user rights are provided for, they are necessary and proportionate; onward transfer rules for data that subsequently leaves the UK; and additional safeguards for records of processing, data protection impact assessments, the appointment of data protection officers, and breach notification.

"Robust rules require robust enforcement, and the UK's framework provides for effective administrative and judicial redress for data subjects in the UK and the EU," said the government.

It pointed out the Information Commissioner's Office's track record of strong regulation and tough sanctions on offenders since the GDPR came into force, and robust laws pertaining to law enforcement and national security, in particular the controversial Investigatory Powers Act of 2016.

It also cited the much-criticised £1.9bn National Cyber Security Strategy, alongside the Centre for Data Ethics and Innovation and Office for Artificial Intelligence as further evidence that the UK was to be taken seriously on data security.

"The UK puts data protection and trust at the heart of our digitised society," said the government. "Our ongoing ability to do this will require a world-leading and global response that sees us work in tandem, at a domestic and international level, to uphold strong data protection standards that enable the societal and economic promise of data while safeguarding rights and protections.

"The UK stands ready to offer further clarifications throughout the assessment process and looks forward to an open dialogue with the Commission." ■

UK SPIES HUNT DOWN COVID-19 THREATS

The UK's National Cyber Security Centre (NCSC) has stepped in to remove malicious and phishing websites linked to Covid-19 scams, but warned that attacks could increase if the outbreak does.

The GCHQ body said that phishing efforts using the Coronavirus as a lure have led to victims losing money and sensitive data across Europe.

It urged businesses and consumers to consult its advice on email scams and dealing with malware to better insulate them from the threat of ransomware, credential theft and fraud.

"The NCSC has seen an increase in the registration of web pages relating to the Coronavirus suggesting that cyber-criminals are likely to be taking advantage of the outbreak," it said.

"Continued global susceptibility to phishing will probably make this approach a persistent and attractive technique for cyber-criminals. Moreover, if the outbreak intensifies, it is highly likely that the volume of such attacks will rise."

Security vendors have been sounding the alarm over phishing attacks for more than a month. Emails are often spoofed to appear as if sent from the World Health Organisation (WHO), the US Center for Disease Control (CDC) or other official bodies, and claim to contain new information on the outbreak in an attachment or via a link.

Some are laden with malware while others request the user enter their email and password, Outlook log-ins or other credentials to proceed. There are also reports, cited by the NCSC, of fraudsters requesting Bitcoin donations to fund a fake vaccine, and even scam sites selling fake antiviral equipment.

"We know that cyber-criminals are opportunistic and will look to exploit people's fears, and this has

undoubtedly been the case with the Coronavirus outbreak," said NCSC director of operations, Paul Chichester.

"Our advice to the public is to follow our guidance, which includes everything from password advice to spotting suspect emails. In the event that someone does fall victim to a phishing attempt, they should look to report this to Action Fraud as soon as possible." ■

CLOUD DATABASE LEAK EXPOSES 425GB OF SMALL BUSINESS FINANCIAL DATA

Over half a million highly sensitive legal and financial documents have been leaked online by a US loans company after another cloud configuration error.

Security researchers at vpnMentor led by Noam Rotem found the database in an unsecured Amazon Web Services (AWS) S3 bucket at the end of December.

It appears to be linked to a smartphone app known as MCA Wizard, developed by New York-based fintechs Advantage Capital Funding and Argus Capital Funding,

To be continued on page 21

which vpnMentor claimed were likely owned by the same company.

They are said to provide "merchant cash advances" (MCAs): controversial high-interest loans for small businesses and start-ups.

However, although the database URL contained the words "MCA Wizard," the app is no longer available and most files bore no relation to the project. Even as the researchers discovered and tried to contact the firms, without success, new files were apparently being uploaded to the database.

The 425GB trove contained highly sensitive customer information including credit reports, bank statements, driver's licenses, Social Security info, tax returns, scanned checks, purchase orders, and much more.

With this information, attackers could launch highly convincing phishing attacks, attempt check and financial fraud, target victim companies with malware, or even sell the data on the dark web, warned vpnMentor. The leak could even be investigated under the new California Consumer Privacy Act (CCPA), it claimed.

"This leak raises serious credibility and trust issues for Advantage and Argus. By not sufficiently securing this database and revealing so much information, they have compromised the safety, privacy, and security of their clients, partners, and customers," the firm said.

"Those affected may take action against Advantage and Argus for doing so, either from ceasing to do business with either company or possibly pursuing legal actions. Both would result in considerable loss of clients, contracts, business relationships, and ultimately, revenue."

After receiving no reply from the database owners, the researchers went direct to AWS, which promptly corrected the privacy snafu on January 9. ■

NORSK HYDRO OUTAGE MAY HAVE BEEN DESTRUCTIVE STATE ATTACK

The crippling ransomware attack on Norsk Hydro may have been a state-backed attempt to disrupt rather than extort money, and as such provides a "blueprint" for how similar future campaigns may work, Dragos has warned. The security vendor's principal adversary hunter, Joe Slowik, claimed in a new report that the new version of LockerGoga seen in the attack on the Norwegian aluminium giant last year could be a taste of things to come on the cyber-warfare battle front.

While previous state-sponsored destructive ransomware efforts like NotPetya can at best be described as a "blunt tool," the Norsk Hydro attack was more subtly disruptive, he said.

For example, the new version of the ransomware seen in the latter attack appeared "to work at cross-purposes to monetise the infection." Local user and administrator account passwords were changed to the same hard-coded value, the system network card was disabled and all logged-in users were forcibly logged out.

"The above chain of events means that systems were not only encrypted but became inaccessible. Even viewing the ransom note associated with the event would require additional work, such as forensically imaging the machine to recover the note from disc or analysing the malware," Slowik explained. "While viewing ransom information is certainly possible, such items seem curious and counterproductive for efficient monetisation."

Adding further deniability for state hackers is the fact that financially motivated ransomware attacks are taking place with increasing frequency today, providing perfect cover for those who want to use modified versions of the powerful malware already in use, he continued. "As ransomware has evolved from wildly propagating host-specific infections to more deliberate network compromise, malicious state-directed entities now have a new and valuable option for future disruptive operations," Slowik concluded.

"The combination of efficacy (when properly implemented, deniability (due to continued widespread criminal activity), and specificity (as self-propagation gives way to precise network compromise) enables selective and controlled targeting of entities for disruption and effective IT-based destruction."

Tackling this challenge will require greater industry-wide information-sharing, a rethink on the traditional bifurcation between criminal and state-sponsored activity, and an update of related economic modelling, the report claimed. ■

KASPERSKY, BITDEFENDER MAKE PRODUCTS FREE TO NHS

Security suppliers Kaspersky and Bitdefender have both announced free availability of various cybersecurity products and services to healthcare organisations struggling to cope with the Covid-19 coronavirus crisis.

Continuity of operations and data protection put constant pressure on the health service, but now that such organisations find themselves at the frontline of the global emergency, protecting critical systems has become even more of a priority than usual.

As previously reported by Computer Weekly, there has been no let-up in cyber criminal activity targeting hospitals and others operating in the healthcare industry since the crisis began. One victim, a UK-based medical research company, was attacked using Maze ransomware, breaking a promise by the group behind Maze not to attack healthcare organisations at this time.

In Kaspersky's case, the offer extends to free availability of its core endpoint security product lines for six months. These include Kaspersky Endpoint Security Cloud Plus, Kaspersky Security for Microsoft Office 365, Kaspersky Endpoint Security for Business Advanced, and Kaspersky Hybrid Cloud Security. Customers can contact their reseller or business partner, or Kaspersky itself.

Bitdefender, meanwhile, is making its enterprise-grade, end-to-end protection services available without charge to healthcare customers until the end of June 2020. Customers can find out more about its offer on its website.

"In this critical situation, healthcare institutions are under immense pressure and carry huge responsibility while saving people's lives and fighting against the infection," said Evgeniya Naumova, global sales network vice-president at Kaspersky. "Doctors, nurses and all medical staff take on most of the load and therefore need any support possible. We feel it is our duty to support the medical community.

"In order to help these organisations focus on what matters most, we now offer healthcare institutions free licences for key Kaspersky corporate products for a six-month period."

Bitdefender CEO Florin Talpes said: "Hackers have acted opportunistically and unethically, taking advantage of this time of uncertainty to deliver malware, conduct phishing, and perform online fraud against the organisations affected most.

"We are thankful for the work of healthcare professionals worldwide and aim to support them by providing protection for their organisations' sensitive information in a way that assures operational continuity and lets them focus on treating patients and slowing the spread of this virus."

Even though doctors and nurses are under immense pressure, Kaspersky said it was still important for hospitals and healthcare organisations to follow basic cybersecurity best practice. End-users still need to be educated on security hygiene, covering passwords, how to spot phishing emails, and so on.

It is also the right time for NHS IT and security teams to thoroughly audit their existing protection systems, making sure they are patched and properly configured. Firewalls should be enabled and beefed up where possible, endpoints will need to be protected, especially those belonging to doctors and nurses, and particular attention should be paid to protecting systems from ransomware, to which hospitals especially are acutely vulnerable.

Perhaps most critically, any connected medical devices, such as ventilators, must be properly configured and updated, because any failures will be life-threatening. ■

SANS OFFERS FREE KIT TO SECURE HOME WORKERS

The SANS Institute has produced a training kit and additional resources designed to offer organisations, individuals and parents some best practice advice on working from home securely, as the Covid-19 pandemic spreads.

The information security training provider claimed its Security Awareness Work-from-Home Deployment Kit will help to fill knowledge gaps as organisations rapidly transition to new distributed working set-ups.

"For many businesses, managing an entirely remote workforce is completely new, which means they may lack the processes, policies and technologies that enable employees to work from home safely and securely," it argued. "In addition, many employees may be unfamiliar or uncomfortable with the idea of working from home."

The home working kit for employers highlights three main risks to remote employees: social engineering, weak passwords and unpatched machines. Other potential challenges to consider include incident detection and response, Wi-Fi security, VPNs, remote workers outside the home and guests/family members who want to use work devices.

It recommends business leaders cooperate closely with their IT security and comms teams to roll-out their remote working strategy, and urges effort be made to create a forum where users can have their questions answered and report incidents, preferably in real-time. Alongside the deployment guide there's a factsheet for micro-businesses or sole traders working from home, which outlines five key steps to protect against major cyber-threats.

There are also resources for parents faced with the prospect of children using the internet at home for several weeks whilst schools are closed.

"The key advice is: be suspicious of any emails trying to create a sense of urgency to click on a link or send information; take steps to protect your home Wi-Fi, changing default passwords and restricting access," SANS director of security awareness, Lance Spitzner, told Infosecurity.

"Also create strong passwords on any websites you use, make sure any device is running the latest software, and don't let family and friends use work devices."

Multiple security and tech vendors are stepping in to help businesses that may be struggling to support remote working.

Trend Micro is offering six-months free access to its consumer security product, Trend Micro Maximum Security, while SentinelOne is providing free use of its endpoint security platform until mid-May. ■

HORANGI RAISES US$20M TO EXPAND ITS MARKET LEADERSHIP IN SOUTHEAST ASIA

Horangi, a Singapore-based cybersecurity company which provides solutions to industry leaders across Southeast Asia, announced a US$20 million fundraise in a Series B round, led by Southeast Asian private equity firm, Provident Growth, which has funded companies like Indonesian ride-hailing platform GoJek and travel e-commerce Traveloka. Other participants in this funding round include Singapore's Monk's Hill Ventures, Australian venture capital firm Right Click Capital, and Southeast Asia's leading venture debt fund, Genesis Alternative Ventures. This round brings Horangi's total funding to US $23.1 million, including their Series A round in November 2017.

Horangi will use the funds to support its expansion plan in Southeast Asia as it strengthens its position as the region's leading cybersecurity company. This includes enhancing its cloud security product, Warden, integrating its market-leading cybersecurity expertise and insights, as well as infusing artificial intelligence and machine learning technologies in order to help organisations stay ahead of advanced threats. Horangi will also double its staff to 160 across the region, and significantly grow its presence in Singapore and Indonesia, where demand has been highest.

"Southeast Asia is one of the fastest-growing economies and digitising rapidly, but due to the shortage of security expertise in the region, organisations are increasingly turning to security experts like Horangi. This is especially prevalent in Indonesia, where we have been focused on since 2016. Having a strong team, local insights and technology capabilities allow us to partner with strategic investors to help propel our next growth stage," said Horangi CEO and Co-Founder Paul Hadjy.

George Do, Chief Information Security Officer of Gojek said, "The challenges that the region face in this age of digitalisation needs to be met with a holistic cybersecurity strategy that requires a security-first mindset. We're lucky to be partnering with Horangi to reinforce our commitment to the safety of our customers, driver partners, merchants, service providers, and business partners. Gojek has grown into the biggest on-demand application platform in Indonesia and Southeast Asia, its application is accessed by more than 30 million users each month in Southeast Asia."

Since its launch in 2016 by former Palantir cybersecurity experts Paul Hadjy and Lee Sult, Horangi has worked with over 200 customers, including Gojek, Ninja Van, Shopback, Tiket and Property Guru, to provide best-in-class cybersecurity solutions.

Horangi's cloud security product — Warden — protects organisations using public cloud infrastructure from critical security threats and compliance violations in the cloud. Warden is featured on the AWS Marketplace and Horangi is a Select tier partner in the Amazon Web Services Partner Network. Horangi's services, which include Penetration Testing and vCISO, empower organisations of all sizes to stay ahead of the most sophisticated cyber threats. Horangi recently announced that it became Tokio Marine Insurance Singapore's (TMiS) first cybersecurity partner in the Asia-Pacific region.

Michael Aw, Partner at Provident Growth shared, "Our investment in Horangi is in line with Provident Growth's investment philosophy to back growth-stage technology companies. Horangi has a stellar founding team with many years of cybersecurity experience, and has established a strong brand among reputable technology customers and a market-leading position in its core markets."

Provident Growth will support Horangi in realising the full potential of its existing cybersecurity businesses while investing further in enhancing its technology capabilities. Horangi will also be able to leverage on Provident Growth's strong operating experience, extensive network and relationships in Southeast Asia.

Dr Jeremy Loh, Managing Partner at Genesis Alternative Ventures which has supported Horangi since their Series A funding said, "As Horangi scales its business, choosing a venture lender who is committed and understands the business is critical. It's not only about access to capital, but also the flexibility and the invaluable network that Genesis brings along." ■

NTT LTD. RECOGNISED AS A LEADER IN IDC MARKETSCAPE

NTT Ltd., a world-leading global technology services provider, has been named as a Leader in the IDC MarketScape: Asia/Pacific Managed Security Services (MSS) 2020 Vendor Assessment (doc #AP45547820, February 2020). The report noted that customers recognised NTT for its strategic business partnership approach.

The report, which evaluated NTT Ltd. along with 19 MSS providers, noted that NTT Ltd. offers some of the most comprehensive MSS portfolios with its biggest revenue generators in the region spanning threat detection and managed network services. The latest recognition marks the fourth consecutive time NTT Ltd. has been identified as an industry leader among Asia/Pacific MSS providers.

Following the integration of 31 brands and companies, including NTT Communications, Dimension Data, and NTT Security in July 2019, NTT Ltd. is now one of the largest technology service providers worldwide. It is also one of the largest security service providers in Asia/Pacific, with a direct presence in 17 countries in this region. NTT Ltd. leverages its heritage and expertise in networking, data centres and the cloud to help organisations become secure by design as they look to innovate in the digital transformation era.

As more applications and workloads are created and hosted in cloud environments, the report also credits NTT Ltd. for its high proficiency in cloud-based security services and managed cloud security. It also highlights NTT Ltd.'s expertise in predictive threat detection and its Cyber Threat Intelligence (CTI) framework, operationalised by its Global Threat Intelligence Center (GTIC) team. What's more, customer feedback has shown continuous improvement in NTT Ltd.'s service delivery, and how its engagement has evolved from being a service provider-customer relationship to a strategic business partnership.

"The continued recognition as a 'Leader' in the IDC MarketScape for Asia/Pacific MSS is an affirmation of NTT Ltd.'s cybersecurity capabilities and consulting-led approach," said Matthew Gyde, CEO Security at NTT Ltd. "With the ever-evolving cybersecurity landscape and increasing security risks, businesses are looking to strategic partners for innovative solutions to bolster their cyber resilience. Predictive threat intelligence, in particular, is expected to reach new heights. To provide clients with timely and actionable threat detection and threat intelligence, NTT Ltd. remains committed to improving its service delivery standards while investing in R&D to develop advanced analysis techniques and proprietary tools."

With a global footprint of Security Operations Centers (SOCs) and R&D centres, and a comprehensive view of the

dark web, NTT Ltd. is recognised for its visibility into a vast portion of the world's internet traffic. This gives NTT Ltd. access to log, event, attack, incident and vulnerability data, allowing it to gather threat intelligence to help clients detect emerging threats, mitigate security risks and respond to breaches faster.

Gyde adds, "We are constantly looking at what we can do better and how we can provide the best value to our clients. For example, around 75% of the threats detected in our SOCs are now orchestrated by supervised machine learning and threat intelligence. Our security experts use algorithms to recognise patterns, identify anomalies, and automatically orchestrate security controls. Embedding this level of intelligence into infrastructure and applications is a top priority for organisations."

"Of course, organisations can never be 100% protected from a cyber attack, but we can help them take a proactive approach by putting cybersecurity at the core of their business. NTT Ltd.'s expertise in advanced security services, and reputation as a leading MSS provider, will ensure its clients are putting the right protection in place from the start – across business process, technology, services and people," concludes Gyde. ■

SINGAPORE AMONG WORLD'S TOP SOURCES OF ONLINE THREATS

Singapore remained a hotbed for originating cyber attacks in 2019, falling only two places from the year before to rank 10th globally in a Kaspersky study.

The cyber security company said it had uncovered more than 11 million attacks from servers hosted in Singapore last year, representing a 150% decrease over 2018.

The number of web threats, or malware targeting internet users, however, remained significant in Singapore. Kaspersky said it detected 4,657,235 web threats in the city-state, putting it at 157th globally, a regression of only one position compared to the year before.

In Southeast Asia, the top four attack vectors of web threats were unintentional downloads of certain files from the internet, malicious attachments from online email services, browser extensions activity, and malicious communications with command and control (C2C) servers.

While web-mining activity fell at the beginning of the year in Southeast Asia due to declining interest in cryptocurrencies, Kaspersky observed a significant growth in the number of online skimmers, using malware to steal user account information such as logins and passwords from infected computers.

"Across the region, Singapore has performed well in terms of maintaining its high position for having the least number of cyber threats blocked relative to its neighbours, regardless of whether they are internet-borne or local in nature," said Yeo Siang Tiong, general manager at Kaspersky Southeast Asia.

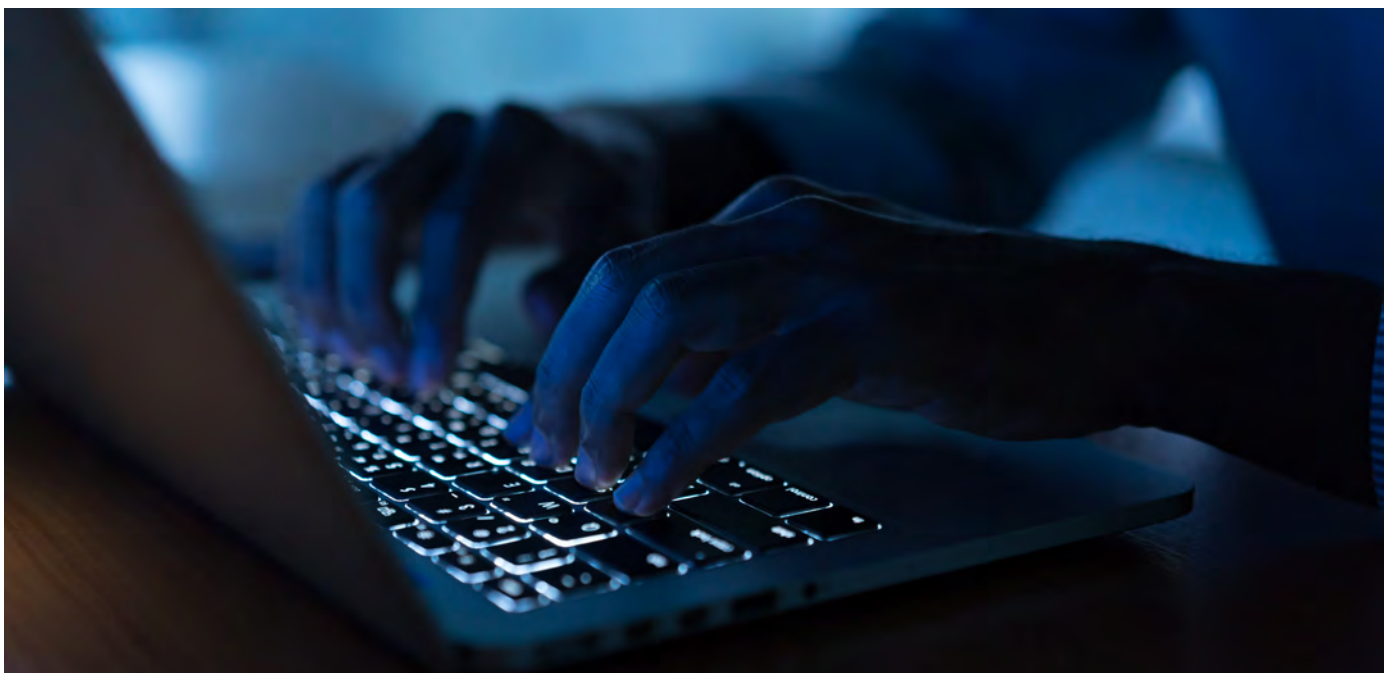
"These noteworthy results are commendable, and we have to give a nod on how public and private institutions in the country are working together actively to keep the digital aspect of the Republic safe and secured," he added.

Singapore's cyber security landscape ended on a sombre note last year. Yeo said the spate of cyber security incidents, including the leakage of personal data of 2,400 Ministry of Defence personnel and the Sephora hack, showed that the city-state continues to be a key target for cyber criminals.

"The government is undoubtedly stepping up its efforts to build up its defences. For our part, we renewed our commitment to sharing threat intelligence with Interpol last year, as we believe that building cyber security capacity must be a shared responsibility," Yeo added.

In February 2020, the Singapore government said it would set aside S$1bn over the next three years to build up its cyber and data security capabilities, to safeguard citizens' data and critical information infrastructure (CII) systems.

Noting that Singapore must be prepared to deal with cyber threats as digitisation becomes more pervasive, Singapore deputy prime minister and finance minister Heng Swee Keat said the Cyber Security Agency (CSA) is preparing measures for the next level of cyber security with the



To be continued on page 27

growing use of artificial intelligence (AI), cloud computing and the internet of things (IoT).

The budget announcement comes on the back of a CSA masterplan unveiled in October 2019 to help secure operational technology (OT) systems used in CII sectors, including transportation, energy and water. Developed together with industry partners, the masterplan details the development of capabilities to secure OT systems, along with plans to set up an OT cyber security information sharing and analysis centre.

Meanwhile, the CSA is also introducing the Cybersecurity Labelling Scheme (CLS) this year for network-connected smart devices. The first of its kind in the Asia-Pacific region, the scheme will provide different levels of cyber security ratings to help consumers make informed choices about the security features of the smart devices they purchase.

As a start, CSA will introduce the CLS to Wi-Fi routers and smart home hubs, which will be assessed on security requirements such as ensuring unique default passwords, adherence to security-by-design principles and resistance to basic penetration testing. With the scheme, which will be aligned to global security standards for consumer IoT products, the CSA hopes to incentivise manufacturers and product suppliers to develop products with recognised and improved security features. ■

IDEMIA AND JAC TO SUCCESSFULLY TEST FRICTIONLESS BIOMETRIC ACCESS TECHNOLOGY

IDEMIA, the global leader in Augmented Identity and Japan Aerospace Corporation (JAC) partnered to demonstrate a proof of concept with MorphoWave™ Compact, a unique award-winning access control biometric device.

A first in Japan, the biometric access technology was successfully tested at Level5 stadium in Fukuoka during the final match of the J2 League between Avispa Fukuoka and Kagoshima United Football Club at the end of 2019.

MorphoWave™ Compact enables four fingerprints to be read in less than one second by a wave of the hand across the device. This biometric access solution enables the stadium to combine speed and convenience with a high level of security within its high traffic environment.

Two use cases were tested during the game:

1. Ticketless / handsfree admission: pre-registered customers were able to enter the stadium by biometric authentication without a physical ticket
2. Verifying the identity of the customer by a wave of the hand on the biometric terminal at the food and beverage pick-up counter.

"Our goal is to enable frictionless access everywhere without compromising security," said Nobuyoshi Nezu, Managing Director and Vice President of Sales for IDEMIA Japan. "IDEMIA has developed MorphoWave™ Compact, a touchless fingerprint device that enables this, by combining a high level of biometric security with a unique user experience, convenience and speed, which is what environments like a stadium need. We are excited to partner with Japan Aerospace Corporation on this very promising case and look forward to a full rollout of our MorphoWave™ devices at Level5 Stadium." ■

CLOUDFLARE AND ALIBABA CLOUD COLLABORATE ON EXPANSION OF BANDWIDTH ALLIANCE

Cloudflare, Inc. (NYSE: NET), the security, performance, and reliability company helping to build a better Internet, announced that it has expanded the Bandwidth Alliance by partnering with Alibaba Cloud, the data intelligence backbone of Alibaba Group.

The Bandwidth Alliance, launched in September 2018, is a group of forward-thinking cloud and networking companies that are committed to discounting or waiving data transfer fees (also known as bandwidth fees) for shared customers.

The Bandwidth Alliance now includes 20 partners, all committed to providing the most performant and cost-efficient experience for mutual customers.

"We launched the Bandwidth Alliance to give our customers a faster, more secure, and more reliable Internet, without the awful fees that have historically bogged them down," said Arjunan Rajeswaran, Head of Strategic Partnerships at Cloudflare. "Alibaba Cloud has built an impressive business that considers its customers first, and together, we will give our joint customers the best Internet experience possible."

By joining the Bandwidth Alliance, customers using both Alibaba Cloud Object Storage, and Cloudflare products, will have their data egress fees waived outside mainland China if OSS products are purchased from alibabacloud.com.
"In addition to waiving the egress fee, Alibaba Cloud will also waive up to 100 million API requests, and 10TB image processing fees for all customers in regions outside of China after joining the Bandwidth Alliance," said Alex Chen, Alibaba Cloud Senior Director of Product Management. "Alibaba Cloud's initiative of the elimination of 'request fees' is an industry game changer. The combined solution will pass on massive savings to our customers, and at the same time, eliminate complexity in managing storage cost."

Alibaba Cloud continues to champion millions of businesses in more than 21 regions and countries through world-class infrastructure, advanced analytics tools, and a thriving ecosystem. Its hybrid cloud model services enterprises, developers, and government organisations around the world, and makes them a valuable partner within the Bandwidth Alliance.

Cloudflare has long had an international presence, with co-location facilities in 200 cities across more than 90 countries, including China.

Cloudflare also recently partnered with Cherry Servers, a provider of bare metal cloud services in Europe, as part of the Bandwidth Alliance. ■

TÜV RHEINLAND SIGNS STRATEGIC QUALITY ALLIANCE AGREEMENT WITH KAOLA

On March 11, TÜV Rheinland Group was invited by the Alibaba Group to attend its cloud contract-signing ceremony for the Kaola Quality Alliance. Yushun Wong, CEO and President of TÜV Rheinland Greater China, attended the ceremony and delivered an online speech as the representative for testing, inspection, and certification service providers.

Government officials including Kun Wang, Secretary-General, China Association for Consumer Products Quality and Safety Promotion, representatives from the Kaola platform, and testing service providers joined in witnessing the "cloud signing" of the "Quality Alliance Strategic Cooperation Agreement" between members of the Quality Alliance and Kaola. The agreement paves the way for in-depth cooperation in international certification and review of merchants, international product quality control, supply chain quality control, warehouse and logistics management, definition of quality standards, and the upgrading of quality inspection capabilities.

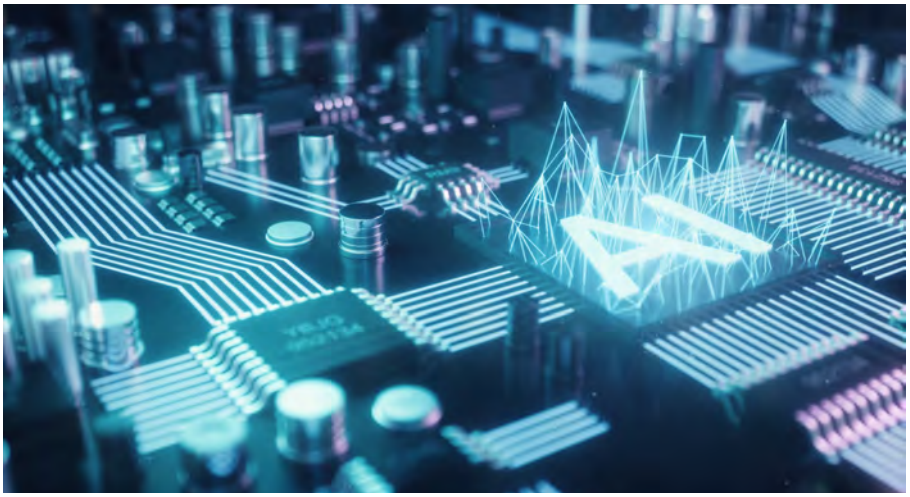
In his speech, Yushun Wong said: "The establishment of the Quality Alliance embodies Ali's accountability as a leading global e-commerce platform, and its commitment to high quality developments in the industry. As a member of the Quality Alliance, TÜV Rheinland is drawing upon more than a century of technical expertise, a comprehensive global service network, and extensive experience in the e-commerce sector to work with other partners in supporting the sustainable development of international e-commerce and improving quality of life for Chinese consumers."

The introduction of favorable national policies for international e-commerce exports and strong support from the international e-commerce industry has led to international e-commerce exports becoming the "black horse" of foreign trade. The sector is now an important component of economic growth in China. The next step is to improve the consumer experience on the platform and regulate issues relating to international product quality, supply chains, and warehousing. These issues have become bottlenecks holding back the development of international e-commerce. TÜV Rheinland has been working closely with the Alibaba Group on its e-commerce platforms for 8 years. The two sides have established a solid foundation for cooperation on standards, testing and inspection, assessment, and certification. The professional quality certifications offered by TÜV Rheinland in each sector are also effective in providing product guarantees that build trust between the consumer and the enterprise.

According to the "Kaola Quality Alliance Strategic Cooperation Agreement," TÜV Rheinland will continue to exploit its technical advantages by helping Kaola, a part of the Alibaba Group, establish a foundation cooperation mechanism for the Quality Alliance based on informatisation and "big data" application products. Resources from both parties will be combined to solve problems related to standards, testing, assessment, and certification supply and demand. The resolving of industry pain-points and upgrading of transnational supervision will be used to realise the standardisation of imported products and services.

TÜV Rheinland was set up in China more than 30 years ago. Now, in addition to providing the full spectrum of quality and safety services to foreign buyers, it also provides Chinese buyers with professional technical support as well as solutions that conform to local standards. TÜV Rheinland has established a business relationship with all the large e-commerce platforms in China, helping them enhance their quality. In the future, TÜV Rheinland will continue to apply its professional strengths and build a bridge for "Go Out" and "Come In" two-way cooperation with Chinese companies. ■

YOKOGAWA ACQUIRES DANISH STARTUP GRAZPER TECHNOLOGIES, SPECIALISTS IN AI FOR IMAGE ANALYTICS



Yokogawa Electric Corporation (TOKYO: 6841) announces that on March 20, 2020, it completed the acquisition of all shares in Denmark-based Grazper Technologies ApS (Grazper), as mutually agreed. Grazper has developed advanced artificial intelligence (AI) technologies for analysing images, and Yokogawa aims to leverage these technologies within its various existing businesses and to develop new industrial AI solutions.

Recent advances in deep learning and related technologies have enabled the practical application of AI in industry, and it is expected that as image identification and data forecasting accuracy continue to improve, the use of AI will only expand further. In particular, by improving the recognition accuracy for moving imagery, it becomes possible to observe the overall environment and context of the whole image, opening up new applications in the security field and for image analysis and robot operations on production lines.

Grazper is a venture company founded in Copenhagen, Denmark in 2015, and later funded by Danish venture capital firm Promentum Equity Partners. It possesses advanced AI-based technologies for image analysis, and one notable strength is a solution that allows AI software to run efficiently on a field-programmable gate array (FPGA*), a type of integrated circuit. The software employs image recognition methodologies that have been theorised using algorithms and 3D modeling, and it can be operated with limited computing resources.

Yokogawa is developing and providing AI-based solutions for plants and public infrastructure projects.

Acquiring Grazper's technology will enable the company to provide solutions that use AI for image analysis, such as capturing image information for robots, detecting abnormalities at plants, and monitoring security using cameras. As a first step, Yokogawa's subsidiary, amnimo Inc., will embed Grazper's FPGA IP core into its Edge Gateway industrial LTE gateway, which is currently under development. This will make possible solutions for smart city projects and security applications targeting airports and railways.

As part of Yokogawa's Transformation 2020 mid-term business plan, the company is working with customers on digital transformation initiatives that utilise technologies such as AI and IoT. Through this acquisition and the addition of new technology, Yokogawa will create new value by co-innovating with customers. ■

* *A device that allows the immediate rewriting of the logic circuit design in the hardware language*

COHESITY EXPANDS ASIA PACIFIC OPERATIONS TO SUPPORT GROWING CUSTOMER DEMAND

Cohesity announced a significant expansion within the Asia Pacific and Japan (APJ) region, as the company extends its innovative data management capabilities in India, Hong Kong, and Taiwan. The company has hired industry veterans to lead those markets and has invested in sales, marketing, and engineering. Cohesity has also hired accomplished channel and technology leaders with pan-APJ responsibilities.

Cohesity radically simplifies the way companies back up, manage, and extract value from their data and these new leaders will play a key role in empowering customers and partners to embrace a software-defined, modern approach to data management.

Specifically, Cohesity has hired Marcus Loh as chief technology officer (CTO) and Les Mansour as head of channels for APJ. The company has also appointed Sunil Brid as head of India as well as Linda Hui, who will lead Cohesity's business in Hong Kong and Taiwan.

The announcement follows recent appointments of Sheena Chin as head of Cohesity's ASEAN business and Steve Coad, who has oversight for Cohesity's expanding business in Australia and New Zealand.

This expansion is taking place as demand for Cohesity's data management solutions continues to rise globally and across Asia Pacific. In the Asia Pacific region, Cohesity's software bookings have increased by more than 100 percent when comparing the company's most recent quarter (Q2 FY 20) with the same time period last year (Q2 FY 19). And the number of customers that have deployed Cohesity in the region rose by nearly 250 percent in that same time period, while the number of active booking partners in the region grew by 190 percent.

"We are excited to bring on a team of seasoned executives that can help organisations and partners across Asia Pacific embrace a modern approach to data management," said William Ho, vice president of sales, Asia Pacific, Cohesity. "Organisations are looking for alternatives to legacy products and want to embrace software that makes it a snap to back up, manage, and extract value from data. That's what Cohesity provides and these leaders will empower more businesses and partners to embrace our unique platform to accelerate digital transformations."

The company's new APJ executives have more than 100 years of combined experience in helping organisations and partners drive business growth utilising cutting-edge enterprise infrastructure and technology.

▪ **Marcus Loh,** based in Singapore, joins Cohesity from Veritas Technologies and brings over 27 years of expertise in enterprise technology. As CTO for the company's Asia Pacific operations, Loh will drive Cohesity's technology strategy in the region.

▪ **Les Mansour** joins as senior director of channels, Asia Pacific and Japan. He will lead all channel operations for Cohesity across APJ. His 25-year career with some of the industry's biggest tech vendors, including Hewlett Packard Enterprise (HPE), Hewlett Packard, Lenovo, and Quantum, has focused mainly on channels, data storage, and business transformation. Mansour will be joined by Danny Wan, who will lead Channels for the ASEAN region. Wan previously led channel teams at Symantec, Pure Storage, and Check Point Software and has been instrumental in helping organisations expand in the ASEAN region.

▪ **Linda Hui** has joined Cohesity as managing director of Hong Kong, Taiwan, and Macau. She brings more than 25 years of experience in enterprise technology and has been instrumental in helping businesses rapidly grow in this region. Previously, she held senior leadership positions at Ruckus and F5 networks.

▪ **Sunil Brid** will lead operations for Cohesity's business in India. He brings over 29 years of sales and management experience, having held senior sales leadership positions with EMC and Hewlett-Packard Enterprise (HPE).

Cohesity also recently announced a significant expansion of its operations in Pune, India, with plans to hire 100 people within the next 18 months. Since Cohesity's entry into the Asia Pacific region in 2018, the company has established operations in Australia, New Zealand, Japan, Hong Kong, Singapore, India, Malaysia, Thailand, and Indonesia. ■

Unraveling Unmanned Aerial Vehicles

By CJ Chia

Drones are becoming increasingly common, and the range of their applications have grown tremendously since the technology was first introduced. In order for widespread use to be viable, the technology must keep improving, but it is also important to tackle the challenge of creating strong but sensible regulations around drone use.

With advances in technology, unmanned aerial vehicles (UAVs)—commonly known as drones—are now more accessible and affordable than ever. Drone technology has come a long way in the past several years; not only are drones easier to get and more commercially viable for practical use than ever before, but their capabilities have also increased.

Air Drone Craze, an Amazon Associate on Amazon's affiliate programme, breaks drone tech into seven different generations; the majority of current drone technology falls into the sixth generation, while higher end professional grade drones are starting to cross over into the seventh.

The breakdown by generation as covered by Air Drone Craze is as follows:

- **Generation 1:** Basic Remote Control Aircraft of all forms

- **Generation 2:** Static Design, Fixed Camera Mount, Video Recording / Still Photos, Manual Piloting Control

- **Generation 3:** Static Design, 2 Axis Gimbals, HD Video, Basic Safety Models, Assisted Piloting

- **Generation 4:** Transformative Designs, 3 Axis Gimbals, 1080P HD Video or Higher Value Instrumentation, Improved Safety Modes, Autopilot Modes

- **Generation 5:** Transformative Designs, 360° Gimbals, 4K Video or Higher Value Instrumentation, Intelligent Piloting Modes

- **Generation 6:** Commercial Suitability, Safety & Regulatory Standards Based Design, Platform & Payload Adaptability, Automated Safety Modes, Intelligent Piloting Models and Full Autonomy, Airspace Aware

- **Generation 7:** Commercial Suitability, Fully Compliant Safety & Regulatory Standards Based Design, Platform & Payload Interchangeability, Automated Safety Modes, Enhanced Intelligent Piloting Models and Full Autonomy, Full Airspace Awareness, Auto Action (takeoff, land, mission execution)

While the technology is not without its shortcomings and flaws, the industry is continually pushing out new innovations, and drones will undoubtedly become safer and more dependable.

Going Unmanned Across Industries

With their rising accessibility, drones are rapidly growing in popularity, and have become central to various business functions, helping organisations accomplish tasks more efficiently and safely in areas which are high-risk or

manpower intensive. Some of these uses are more conventional—we've long heard of drones being used in military applications, and drones being used for aerial photography is not a strange concept to us—but drones are also used in ways that we might not think of immediately. Consider a drone that is used to monitor a large batch of crops, or being employed in search and rescue operations.

Indeed, with the versatility of drones, it sometimes seems like the applications of a drone are limited only by the imagination. Here are some of the ways that drones are employed across different industries according to CB Insights.

▪ **Defense**

According to the Centre for the Study of the Drone at Bard College, US military spending on drone technology has increased about $5 billion annually since 2014. An estimated 95 countries around the world already possess some form of military drone technology, an increase from 60 about 10 years ago.

Military drones are generally designed for surveillance, but also see use in offensive applications, like the use of drones armed with explosives in the conflict on the Gaza strip.

When the military uses drones in areas beyond surveillance, the morality of their usage might come into question; nonetheless, there is hardly any doubt that this is will become more common as more countries consider more ways to keep their soldiers safe.

▪ **Emergency Response**

The increased usage of drones is also affected by the development of other technologies. For example, the development of thermal imaging cameras enables emergency response teams to use drones as a means of identifying victims who might be otherwise difficult or impossible to spot with the naked eye.

In 2017, Land Rover and the Austrian Red Cross partnered to design a special operations vehicle with a roof-mounted, thermal imaging drone. The vehicle includes an integrated landing system, which allows the drone to land atop the vehicle securely even while in motion. This operations vehicle hopes to save lives by speeding up response times.

Other applications include using ambulance drones to deliver defibrillators on demand, a concept that has been tested by Delft University of Technology. This will allow the delivery of critical medical technology that can keep patients in hard-to-reach areas alive while awaiting full medical support, which will dramatically increase survival rates in rural and urban areas around the world.

▪ **Humanitarian Aid And Disaster Relief**

Drones have also proven useful during natural disasters, a natural extension of their usage in emergency response. Drones have been used to assess damage, locate victims, and deliver aid. In the aftermath of Hurricane Harvey in 2017, drones were used to help restore power to areas that were damaged, as well as to survey the damage in flooded areas. Drones were also deployed to assist in search and rescue efforts.

In certain ways, drones are also help teams to try and prevent disasters

Drones have also proven useful during natural disasters, a natural extension of their usage in emergency response. Drones have been used to assess damage, locate victims, and deliver aid.

from even happening in the first place. Surveillance drones with thermal imaging cameras can be deployed to detect abnormal forest temperatures, allowing the identification of areas that are most prone to forest fires, and allowing the identification of fires soon after they begin, which helps first responders to get to work on minimising the impact sooner.

▪ **Conservation**
It's estimated by the World Wildlife Fund that thousands of species go extinct each year. To combat this, conservationists are adopting innovative methods like geospatial imagery and autonomous tracking systems to protect and study our global ecosystems, as well as using drones to detect poachers and enable enforcement teams to react.

At Liverpool John Moores University's School of Natural Sciences, a team is working on an autonomous drone system that will be able to follow endangered species and transmit information about the animals' state to researchers.

Drones also provide a means with which research on animals and their habitat can be conducted without disturbing the animal and their natural habitats. An example of this application is the use of drones like the marine SnotBot by the Ocean Alliance to collect mucus samples from whales.

An Unmanned Approach To Pandemic Response

The ongoing COVID-19 pandemic has highlighted the various strengths of drones when applied to crises of unprecedented scale. With the infectiousness of the disease, it is ideal that human-to-human contact is minimised. Japanese company Terra Drone obtained the first urban drone delivery license issued by the Civil Aviation Administration of China, and was able to transport medical and other supplies from Xinchang County's disease control centre to the Xinchang County People's Hospital without exposing delivery drivers to the risk of infection. According to reports by GPS World, the use of drones speeds up transport by 50% compared to road transportation, meaning that deliveries are more timely while eliminating the risk to human drivers.

Other uses in China included the deployment of more than 100 drones to many Chinese cities in order to patrol areas and observe crowds and traffic more efficiently, as well as to broadcast information to a larger area than a traditional loudspeaker can cover. Using drones equipped with thermal sensors, China's eastern city of Nanjing used drones to check temperatures of people under self-quarantine without the need for direct contact between medical personnel and people who might have had the disease. While there was some debate on whether or not this method of temperature checking is as accurate as normal thermometers, this novel solution no doubt provided a safer way to manage the pandemic when used together with other measures.

In Spain, the military used DJI agricultural drones to spray disinfectant in the fight against COVID-19. These drones were used by the Spanish Military Emergency Unit (UME) to disinfect large areas outdoors as well as inside big objects, while simultaneously reducing the risk of emergency personnel being infected by the pathogen.

Regulating No Man's Land

The versatile applications of drone technology during COVID-19 is further evidence of the usefulness of drones when applied as a creative solution to challenging situations. As the technology develops, there is no doubt that drones will become increasingly common in many industries, as well as amongst individuals. This can be a good thing, but brings with it challenges in the form of new security risks.

A critical aspect of the success of making widespread drone use a reality are the regulatory bodies. Currently, most regulations require the drone operator to apply for a permit to fly the drone at a specified time, and this permit to fly often comes with restrictions on the size of the drone and the maximum height to which it can be flown. Perhaps one of the most limiting rules when it comes to flying a drone is that they must be kept in the operators' line of sight at all times.

These restrictions limit the applications of drones in many commercial and personal aspects; if businesses must request permission each time they want to fly a drone beyond an operator's line of sight, it becomes extremely difficult to have apply drone technology in a substantial way commercially.

Still, these restrictions are seen as necessary by many governments due to the nature of drone technology. Unregulated, drones might be used to spy on people in their own apartments or take unauthorised recordings of people in their own private homes. Without height restrictions, drones can potentially endanger lives if a collision with low flying planes were to occur. If bigger drones were to begin running fuel and traveling long distances, there will be an increased risk should the drone fall to the ground or crash into a building.

With the technology still being relatively new and advancing at a rapid pace, it's inevitable that rules and restrictions have become outdated since their implementation. Regulatory bodies will need to play catch-up and consider new ways to regulate drone use in ways that will keep people safe, but allow the technology to be as effective as possible.

This is a work in progress; in the US, federally sponsored projects explore what regulations make sense for drones. But this is a slow, measured process, and it will be several years before regulations support the widespread use of drones in many cities around the world. ■

On The Road Again: AI & IoT Making Public Transit Smarter And More Secure

Internet of Things (IoT) and Artificial Intelligence (AI) have changed the way we interact with each other and the world. Of the markets affected by the trend of going smarter, the transportation industry is one that tops the list.

By Mike Beevor, Field Chief Technologist, Pivot3

As someone who spent more than 200 nights on the road in 2019, using all manner of public transport, it heartened me to see the innovation and development of digital technologies in action, such as improved cameras that can recognise security and behavioural trends, operational or safety-based inefficiencies or even ways of improving the travel experience for passengers. Continued adoption of the Internet of Things and artificial intelligence in 2020 promises to continue to make transit systems safer and more efficient.

Artificial intelligence (AI)-enabled solutions for increased mobility via smart devices has led to the Internet of Things (IoT)-connected world being shaped by the increased demand for transformative technologies, such as the wide range of new sensors capable of recording and analysing everything from shopping habits to air quality. IoT has a significant impact on our daily lives, changing how we interact with each other, how we do business and how we ensure safety.

We see these trends impact a variety of markets, and the transportation industry is at the top of the list. According to Research and Markets, the mass transit security market will register a CAGR of more than 8.7% leading up to 2024. The report found that growing concerns regarding terror attacks and crimes have increased the requirement for infrastructure development for mass transit security and technologies, such as video surveillance and analytics, are in demand to support broad safety initiatives.

Building Intelligence

When we imagine the transit of the future, we're consumed by ideas of hyperloops, driverless vehicles, and almost instantaneous matter transfer — and we're not that far away! But for right now, it is the emergence of digital technologies that will be critical to making everyday services run efficiently.

The very foundation of a transit system should be safety. A focus on safety leads to reduced crime and safer conditions for analysing and helps improve response to potential incidents. And these critical safety functions rely on data.

Safe transit environments are built on information collated from an array of sensors and databases combined with video data and analytics. Facial recognition, behavioural analysis, license plate recognition, and other intelligent solutions are all becoming more commonplace, which means that effectively collecting, analysing, storing and acting on all of this information in real-time is critical to achieving safety and operational goals. That doesn't happen without the proper infrastructure.

The Safe Transit Systems of the Future

While most transit authorities rely on video, security and IoT platforms to better protect and optimise their operations and passengers, these solutions are often decentralised, disconnected, prone to failures and costly to maintain. Additionally, the demand for real-time analytics to improve situational awareness grows as data capture efforts increase. As the volume and collection of data expand, traditional IT infrastructures fall short of fulfilling the demands of these environments.

In addition to effectively monitoring, storing, securing, processing and mobilising data from hundreds and thousands of cameras and sensors, a transit agency's IT infrastructure solution must integrate seamlessly with existing and new IoT technologies. It also must support multi- demands, as well as big data and analytics applications of video-based metadata, including crowd management, traffic monitoring, parking systems and more.

An agile, software-defined infrastructure solution with the flexibility to balance performance, resilience, and scalability can ensure all the elements of a transit system's safety and security environment work together to protect travellers from crime and terrorism and mitigate risk, while simultaneously improving traveller experience.

Safe transit environments are built on information collated from an array of sensors and databases combined with video data and analytics. Facial recognition, behavioural analysis, license plate recognition, and other intelligent solutions are all becoming more commonplace, which means that effectively collecting, analysing, storing and acting on all of this information in real-time is critical to achieving safety and operational goals. That doesn't happen without the proper infrastructure.

Hyperconverged infrastructure (HCI) allows for the consolidation of video management, IoT data collection, video, and data analytics as well as storage, access control, and other related applications onto a single, simple-to-deploy and easy-to-manage industry-standard appliance. HCI platforms eliminate the complexity of separate physical servers and storage and provide a more seamless way to scale the infrastructure as camera or sensor counts grow and analytics demands increase.

Transit security management and IT teams worldwide have to contend with constant security, safety, and operational challenges. They are often tasked with building, deploying and managing a large-scale, distributed security system that must account for critical security services, safety protocols, regulatory and policy compliance, operational efficiencies and changing business needs, all while improving traveller experience and keeping costs in check.

In this extremely dynamic environment, using IoT and video analytics to keep travellers safe needs the assistance of technology, and that technology needs to run on an infrastructure designed to help keep the trains and buses running on time. Given that I am projecting over 200 nights on the road in 2020, I'm thankful for the technologies that keep innovating and making the transit experience safer and sounder. ■

5 Key Developments In IoT For Transportation And Logistics

Key developments in IoT have been transforming the transportation sector in order to gain real-time fleet management wins.

By Mike Jeffs, Chief Commercial Officer, Hark

The Internet of Things (IoT) is becoming prevalent within many different industries, and a new area of growth is being seen, especially in transportation. According to the IDC, the transportation industry has now become the second-largest segment investing in IoT with an approximate spend of $78 billion since 2016.

One of the key areas where this investment has been used is fleet management. IoT-enabled fleet management systems (FMSs) allow companies to receive real-time information of their vehicles, allowing them to make more informed decisions.

Key Developments

1. Real-time tracking: IoT-enabled GPS trackers allow companies to accurately monitor a vehicle's location at all times. The data is transmitted to a central system that sends real-time updates to an internet-enabled mobile device. This allows for quick responses to potential re-routes, avoiding subsequent delays.

2. Smart inventory management: IoT sensors can be implemented across multiple warehouse and distribution centres. These sensors can track quantity of assets in each location alongside monitoring current conditions. This reduces the risk of human error and provides instant insight into the number of goods at each facility.

3. Asset management: IoT can also be used for real-time asset tracking; sensors are used to track individual assets within a consignment to provide regular updates on location as well as other critical readings, such as temperature and humidity in cold chain logistics, and regulated consignments, such as pharmaceuticals. This is an especially vital feature for high-risk or expensive goods that need continuous monitoring in order to protect the asset's integrity. Furthermore, these sensors can act as a form of quality control that provides highly accurate and consistent information to ensure strict health and safety regulations are met.

4. Geo-fencing: Geo-fencing is an advanced form of GPS tracking that uses the coordinates of a particular area to capture the location of a device. It will send instant updates if a driver deviates from the approved route. This reduces the chance of a parcel being lost in transit and of the delivery being delayed, and it can also act as the first line of inquiry in a suspected transport crime.

5. Real-time vehicle diagnostics: In on-the-road (OTR) logistics, vehicle efficiency is monitored in a similar way to an industrial manufacturing facility. You'll find sensors and actuators much like those on a manufacturing line. Similarly, a huge amount of vehicle diagnostic data is generated. This data can be routed and consolidated into onboard computers, serving as an IoT gateway, from which data can be sent to cloud-based servers for analysis and instant decision-making by the fleet owner.

Reap The Rewards

Approximately, $20M was lost last year in revenue due to empty miles. Developments in IoT are allowing businesses to have more control over their fleet operations. Time is saved by choosing the best possible route, and real-time updates allow drivers to avoid congestion, reducing fuel consumption.

Costs can also be reduced by bringing down the number of lost or damaged assets, as well as the percentage of spoilage on any perishable consignments, as alerts are sent immediately when assets go outside specifications.

Environmental Benefits

Transport companies are beginning to consider the environmental benefits IoT can provide. A study of 100 global transportation companies conducted by Inmarsat demonstrated that 44 percent were prioritising environmental monitoring and 65 percent expected to become more sustainable in the future due to IoT implementation.

As the demand for travel continues to increase, so does the level of CO2 emissions, which are expected to increase by 60 percent by 2050. Therefore, companies are expected to reduce their carbon footprint as much as possible and meet the Climate Change Act legislation. This is particularly prevalent for the transportation sector as fleets travel thousands of miles and are a major contributor to CO2 emissions.

Car makers have already been set strict targets that must be met, and they will be fined €95 for every gram of CO2 that exceeds the target. We can expect that it won't be long until logistic companies will be facing similar fines, so it is important to stay ahead of legislation. IoT-enabled technologies give companies the competitive edge to achieve environmental sustainability before regulations are put into place.

Future Predictions Of Smart Transportation

Since Amazon's introduction of their delivery drone, there has been growing discussion around autonomous fleets being the way forward. Drones are not the only option when it comes to autonomous vehicles, and autonomous trucks are very much a viable option, predicted to be a reality by 2030. Rolls Royce has even introduced plans to launch autonomous cargo ships in the same year. In the future, it is a possibility that the entire supply chain will be self-orchestrated.

IoT transportation, from a commercial perspective, is not the only movement; public transportation is predicted to integrate IoT into their operations over the coming years.

McKinsey has recently conducted a research project into future predictions of IoT applications in this field. Some of the key applications mentioned were real-time public transport information, digital payment, autonomous vehicles, intelligent traffic signals, smart parking, and predictive maintenance of the transportation infrastructure.

Each of these ideas are aimed at improving the current infrastructure to make the system more efficient and hopefully more reliable. Although major cities around the world have begun planning IoT implementation, Mckinsey predicts these solutions may only start coming into fruition in the year 2025. ■

Advanced Transportation Initiatives Require Dynamic, Data-Enabled Mapping Systems

Interactive, data-integrated maps can help residents, visitors and city planners by putting all transportation resources into a single, easy-to-access hub of information. Such maps make cities smarter and easier to navigate.

By Jennifer Gombeski, Account Executive at Concept3D

It's safe to say that improving transportation is a priority for most, if not all, municipalities. By 2050, two out of every three people are likely to be living in cities or other urban centres, according to a 2018 United Nations report. Rapidly changing trends in individual transportation—electric bikes, car shares, scooters and concepts like Elon Musk's high-speed tunnel system, are changing the way people move.

Smart Transportation System

The challenge is how to make all of these transportation options available to city residents and visitors and keep them easy-to-use. Advanced transportation initiatives and projects, particularly fast-moving ones like e-scooters, require advanced mapping systems that can keep up and help both municipal transportation professionals and the public maximise the benefits of the options available for getting around.

Every municipality is interested in improving transportation, making it easier for residents to move around efficiently. Digital maps with wayfinding capabilities can play a critical role in presenting transportation options—putting everything that a city has to offer into one easy to use platform. Below are some of the ways a digital map can help simplify and transform transportation within cities.

Ride Sharing

Ride-sharing has changed the way people drive—especially in cities. The sharing economy, peer-to-peer platforms that provide access to shared goods and services, is estimated to be a $335 billion industry in the US by 2025, and the millennial generation is driving most of this growth, according to Forrester Research.

People living in urban areas know they have options aside from outright car ownership. Ride-sharing and vehicle-for-hire services are changing the way people get around. Zipcar, Uber and Lyft are available in all major cities.

With an interactive map, Zipcar pickup and drop off locations can easily be displayed with. Designated pickup and drop-off spots for Ubers and Lyfts can be set and updated at popular locations such as airports, sports complexes or event centres.

These applications can be extremely helpful during major events in urban areas, where crowds of people are gathered for a convention, parade, sporting event or other reason. The map can be rapidly updated with a special event overlay, showing all of the available transportation options, closures and other needs.

A dynamic map can display all of the e-bikes and scooters available throughout the city, as well as pickup and drop-off locations. Once at the pickup or drop off location, people can use the map to find the best routes to get to their final destination.

Scooter and Bike Sharing

Driving and walking are no longer the only options for getting to and from work, especially with the growth of e-scooter sharing and bike-sharing.

A dynamic map can display all of the e-bikes and scooters available throughout the city, as well as pickup and drop-off locations. Once at the pickup or drop off location, people can use the map to find the best routes to get to their final destination.

Public Transportation

Aside from these transportation sharing options, municipalities are focused on increasing the use of public transportation. But, schedules and routes of buses, shuttles and above and underground trains can be overwhelming and frustrating for even the savviest city dweller.

Digital maps that have GIS integration and wayfinding capabilities can help simplify the use of public transportation. With a smartphone, map users can quickly find the nearest train station or bus stop, when the next bus is scheduled to arrive and point-to-point wayfinding instructions for how to get there.

Additionally, city workers can use these maps to send out alerts to the public about any changes to the schedule, breakdowns or emergencies, with estimated times and alternative routes.

Parking

Parking in an urban environment can feel almost impossible at times – with the constant circling around the block looking for an open parking garage, street parking or even free parking. Drivers spend an average of 17 hours a year looking for parking, adding up to an about $345 per driver in wasted time, fuel and emissions.

Digital maps can have different types of parking highlighted for user ease. Additionally, municipalities can go a step further and use digital maps to track open parking spaces across the city. By using RFID tags or other sensor tracking systems, parking availability within a garage or a paid meter on the street can be tracked and then visualised on a map.

Construction

Urban areas are already congested, and construction amplifies this. Construction can be identified on a digital map with up to date information on how the construction may affect traffic patterns.

When it comes to transportation, cities are definitely getting smarter – using interactive maps integrated with dynamic data pipelines can help residents, visitors and event city planners by putting all transportation resources into a single, easy-to-access hub of information. ■

How To Protect Data Privacy In Connected Cars

From monitoring our driving habits to tracking our location, connected cars know our every move. With a black box or event data recorder collecting information inside 96% of automobiles, modern cars are as much a computer as they are a means of transportation.

By JC Gaillard, Founder and Managing Director of Corix Partners

Many drivers and passengers aren't aware of the privacy risks that come along with connected cars. Personal data stored in cars is not always encrypted, or subject to legal restrictions. While details such as seat-belt use, speed, and braking are proving be to useful for insurance companies and law enforcement, personal information including phone contacts and text messages could also be collected without a person's consent.

Connected Cars On Trial

In most countries, police only require probable cause to search vehicles and are not obliged to obtain a warrant before downloading data. The legality of this has already been tested in the courts.

Such cases call on individual courts to decide whether laws dating from before the digital age should be extended to let police gather more information than was originally intended, according to the American Civil Liberties Union. In the absence of universal legal protections, the problem will continue. Every new technology and connected device will bring up the same challenges.

Manufacturers Promise Security

Under regulations like EU GDPR, customers have a right to expect information will remain private unless they expressly give their consent. This puts the responsibility on the vehicle manufacturers to build appropriate security measures that will protect an individual's personal data.

Advanced driver assistance systems (ADAS) such as collision avoiding automatic brake systems provide higher margins for manufacturers. The market for ADAS is expected to grow by more than 10% every year and reach $67 billion by 2025. Manufacturers have every incentive to ensure that these systems comply with data protection regulations and keep sensitive customer data secure.

So far, about 20 carmakers have signed up to build systems featuring built-in security. The plan is to give car owners the ability to manage the data collected in their vehicles, and obtain customer consent to use location and biometric data for marketing.

Encryption Drives Data Protection

To better protect customer data, auto manufacturers will need to introduce encryption technology into their vehicles. VPN software can effectively encrypt data within the vehicle and as it passes over the Internet. By creating an encrypted tunnel for data communications with the auto manufacturer or smart city system, a VPN renders personal data indecipherable and protected from cybercriminals.

Overall, as advances in connected car technology and next generation bandwidth inevitably increase, the number of cases in which personal data in vehicles is analysed without the owner's consent will continue to occur.

To prevent this, manufacturers must take the proper measures to meet data protection laws. Implementing VPN software can ensure that personal information stored in event data recorders and central computer systems is secure and safeguarded from unauthorised parties. ■

How Artificial Intelligence Is Reshaping The Aviation Industry

Advances in AI are reshaping the future for airlines. Application areas include crew management, flight maintenance, ticketing, and passenger identification, and they all centre on one objective: improving the customer experience.

By Sagar Sharma, CTO at Credencys

Business and technology grow hand in hand. Companies that don't leverage technology for the good of their customers or employees don't often last. Today, Airlines are facing a mountain of problems; one of them is the challenge of implementing technological advancements in their business. Emerging technologies, including artificial intelligence, are reshaping the aviation industry.

Artificial intelligence (AI), among other emerging technologies, is still in its initial stages within the aviation business. To date, we can see AI being implemented by airlines for facial recognition, customer Q&A, baggage check-in, factory operation optimisation, and aircraft fuel optimisation.

AI has much more potential than these use cases. It can completely revolutionise the way airlines do business. Below are some of those use cases.

#1 Crew Management

Every day, airline crew managers have the complex task of managing the rosters of an airline's staff, from its flight attendants and pilots, to its engineers. Rescheduling any of the staff can be cumbersome. Multiple factors affect the decision of a manager, such as their availability, credibility, certifications, and qualification.

Jeppensen, a Boeing company, has solved this problem using AI. Their AI-based crew rostering system considers all the aspects mentioned above and manages crew members efficiently.

#2 Flight Maintenance

Aircraft maintenance is a tough task, and if done incorrectly, can cost a fortune to the airline. It requires extensive planning and scheduling. Unplanned aircraft maintenance can result in flight delays or even cancellations. Experts predict that AI, if implemented correctly, can save millions of dollars.

AI-based predictive maintenance is slowly becoming a trend in the global aircraft maintenance market. It has the potential to help the maintenance engineers predict failures before they actually happen. Delta is planning to reduce its number of flight cancellations via AI-based predictive maintenance. According to IBM Watson's TV commercial, AI will also guide on-the-ground repair technicians and guide them through their action items.

#3 Ticketing Systems

Air ticket prices are calculated based on multiple parameters such as oil prices, flight distance, purchase

date, competition, seasonality, the brand value of the airline, and more. Some parameters, such as oil prices, can change daily, which might lead to changes in ticket pricing. Constantly having to calculate this can be time consuming, and can be a complicated process.

An AI algorithm could be the ultimate solution to this problem. Implemented effectively, this solution would be able to help airlines to calculate the most efficient prices for every flight, which will help them remain profitable while providing competitive pricing to their customers.

#4 Passenger Identification

Back in May 2017, Delta Airlines announced that they were going to invest $600,000 into building biometric-based self-service bag drop machines and kiosks for passenger identification. These kiosks will have a built-in camera that will take photos of customers at the time of check-in and match it with their passport. Both the facial recognition kiosks and self-service baggage drop-off machines will leverage machine learning algorithms to carry-out their tasks.

#5 Customer Service

In September 2017, United Airlines announced a collaboration with Amazon's AI, Alexa. A skill named "United" was built for Alexa—once users added the United skill, they could ask common question through voice commands, such as:

- "Alexa, ask United the status of flight 595."
- "Alexa, ask United to check me in for my flight."
- "Alexa, ask United if flight 675 has WiFi."

Alexa's natural language can help to make customers feel as if they are talking to a human sales rep. This is something that can possibly be replicated through different AIs and smart home assistants.

#6 Simplify Communication

Air traffic control (ATC) is one of the most crucial aspects of all flights. In the case of international flights, the communication between a pilot and an air traffic controller can be cross-lingual and cross-cultural. Even though both of them use English for communication, their accent might be different, which can create confusion. For example, it can be difficult for an Indian pilot to understand the heavily accented English of a European controller. Moreover, the communication channels of ATCs are noisy, which makes it more difficult for the pilot to follow.

Thanks to Airbus's AI-Gym program, they have been able to develop a machine learning algorithm that would not only clear the noise in real-time but also provide a full transcript of the controller's audio.

The trend has just begun. As the aviation industry continues to adopt emerging technology like artificial intelligence, they will receive enormous benefits in revenue management, predictive maintenance, flight scheduling, and more. Ultimately, all these benefits will result in one thing, which is at the core of every airline's business: a better customer experience. ■

Artificial intelligence (AI), among other emerging technologies, is still in its initial stages within the aviation business. To date, we can see AI being implemented by airlines for facial recognition, customer Q&A, baggage check-in, factory operation optimisation, and aircraft fuel optimisation.

Finnish Biometric Identity Plans For Seamless Air Travel

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

By Alex Cruickshank, ComputerWeekly.com

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

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

The two organisations worked with a digital identity pilot initiative called Sandbox of Trust, which is aiming to create SisuID, which acts as a portal or aggregator to a variety of different identity documents. Using facial recognition, this potentially means that travellers need never show their identity documents throughout the entirety of their journey, with facial recognition providing authentication every step of the way. Crucially, it's the user who decides which ID information is shared through SisuID.

An earlier study from the International Air Transport Association (IATA) found that 45% of passengers, mainly in the younger generations, are open to using biometric identification for the entire duration of their travel.

According to Jouni Naskali, head of technology and cyber security at Finnair: "As the number of air travellers grows, the industry must find solutions for improving the current processes, and passenger identification is one of the most repetitive, time consuming processes at the

Image by AI Leino from Pixabay

airport. Biometrics has potential for enhancing this process, and Finnair actively explores with different stakeholders how the travel experience could be made more future proof, convenient and secure for our customers."

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

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

"In 2017, we carried out a small-scale test of a biometric identification together with Finnair," said Koski. "The results we got were positive. As many as 30 out of 37 interviewed passengers replied that they would join further pilots or

implementations. The rest said they might join. No one stated that they would not join in future."

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

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

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

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

Data Protection

In accordance with GDPR and other data protection/privacy regulations, there's also work to be done in deciding who controls and processes the data. This isn't easy to resolve, since the data "belongs" to the user, at least in principle. There are also additional considerations when handling the data of passengers travelling outside the Schengen area.

In accordance with GDPR and other data protection/privacy regulations, there's also work to be done in deciding who controls and processes the data. This isn't easy to resolve, since the data "belongs" to the user, at least in principle. There are also additional considerations when handling the data of passengers travelling outside the Schengen area.

In fact, privacy and data security, rather than technology, are likely to be the biggest stumbling blocks to applying the pilot on a large scale, which is partly why there's currently no timetable for implementing seamless whole-journey biometric passenger authentication.

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

Finavia's Naskali agreed: "The project we conducted with Finavia was a pilot where we gathered insight into technical and privacy aspects of deploying biometrics in travel, and at this stage we have no published plans for implementation of biometrics into our processes."

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

Naskali added: "A lot of work is needed to understand current legal and privacy requirements regarding biometrics data usage and user consent and Finnair is actively following many industry workgroups in relation to data security and privacy for these types of applications and the type of standards that should be used and developed."

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

Facial Recognition: Old Myths, New Markets

How to recommend and deploy the technology without drawing the ire of privacy advocates.

By Bill Brennan, Vice President of i-Pro Sensing Solutions (PIPSA) Security Division at Panasonic

Over the past few years, a significant number of people in the United States and around the world have become apprehensive about the prospect of facial recognition technology.

Myths about the technology and its use have pervaded society: It will track us all wherever we went and predict our daily routines; it will make us vulnerable to mistreatment and intrusion by the government; it will leave us vulnerable to private organisations for commercial purposes. While these fears are unfounded when it comes to the technology's use for security, the misconceptions have continued to spread as facial recognition technology has gained traction and found more real-life applications.

By 2010, as image databases began to grow more quickly through the advent of social media and image sharing, further concerns began to circulate about shortfalls in accuracy depending on a person's ethnicity, and the possibility of unjust accusations based on racial profiling.

While facial recognition has become a hot-button topic for privacy advocates, there is no doubting that the technology has exceptional application potential – so much so that it will, without question, continue to proliferate. As the technology evolves to become more accurate, some of the general public's concerns will fade away; and as applications continue to grow well beyond law enforcement, facial recognition will gain even more traction in multiple vertical markets.

However, for security integrators to take advantage of more widespread adoption, they must allay the common fears and misconceptions when it comes to deploying the technology in a security/safety environment.

Debunking the Myths

The reality of facial recognition is very different from the myths; in fact, the level of accuracy has improved enormously in the last 10 years, according to an evaluation performed by the National Institute of Standards and Technology (NIST). The failure rate for searches – meaning that the software failed to find the matching face residing within a database – has dropped from 5% in 2010 to just 0.2% in 2018 – a reduction of 96%.

While the capability of tracking every individual is theoretically not beyond the power of the software, the cost

and bandwidth it would take to do so vastly outweighs any benefits that might exist. The government almost certainly does not want to watch all of us go to the gym, the coffeeshop and the grocery store, rest assured.

Many different industries are beginning to discover specific applications that are relevant to their pain points, and facial recognition is being introduced as a potential solution. The primary use for the technology remains as a solution for law enforcement and other institutions to keep unauthorised or dangerous visitors off-premises.

The Law Enforcement Connection

There is a wide network of facial image databases available to and via the FBI and local law enforcement agencies – including mugshots, the State Department's entire directory of visa and passport pictures, and photos from Departments of Motor Vehicles in at least 22 states. As of October 2020, Americans in 47 states will be required to show either a passport or a new federally compliant Real ID driver's license to board any domestic flight. For non-government users of the technology, databases could include opt-in customers who have provided their photos for a variety of reasons, including security checkpoints, ID access bracelets, VIP club memberships, etc.

All of these databases may also be used to determine the identify of an individual caught on surveillance video who is suspected of a civil or criminal infraction.

Because there are so many image databases available, it is imperative for law enforcement to have absolute certainty when surveillance video of a crime is being matched up in an attempt to identify a perpetrator caught on camera. With the fast-growing advent of deepfakes making it possible to alter video, the chain of custody for evidence must be 100% verifiable.

Vertical Markets: Facial Recognition For Business

Beyond the applications for law enforcement, which could be controversial for some observers,

there is a wide range of industries and organisations using the technology for security, business intelligence and growth.

Retail: With the growth of e-commerce, retail establishments need to step up their game and create better in-store customer experiences in order to maintain traffic and sales. One way they can do this is by using facial recognition to reduce or eliminate checkout lines. Enrolled customers can simply show their face to the camera to make payment instantly. Stores can also use the technology to identify frequent customers as they enter the store, prompting a sales associate to greet them by name. On the security side, facial recognition is already being used to detect known shoplifters as they enter a store, which can deliver immediate and powerful ROI by preventing theft and crime.

Many different industries are beginning to discover specific applications that are relevant to their pain points, and facial recognition is being introduced as a potential solution. The primary use for the technology remains as a solution for law enforcement and other institutions to keep unauthorised or dangerous visitors off-premises.

Airports: Facial recognition can speed up the check-in and boarding process for passengers.

Education: As in many markets, facial recognition can benefit schools with both security and non-security applications. The technology can be used to detect when anyone on a school's watch list – including sex offenders, non-custodial parents, expelled students and teachers who have been fired – enters school grounds. With an alert to school guards or administration, this can reduce the risk of on-site violence. Beyond security, facial recognition can be used to track attendance for students. This form of record keeping is more accurate than sign-in sheets and cannot be falsified by a student's friend covering for their buddies skipping classes.

Gaming: Casinos can greatly benefit from the ability to discover the instant a known cheater enters the premises. They can also benefit from facial recognition in identifying high rollers, so they can receive VIP treatment the moment they arrive. In addition, casinos can create watchlists of individuals who have enrolled in self-exclusion programs in order to deal with their gambling problems, helping to protect gaming establishments from fines for permitting these people to gamble.

Stadiums: Many event venues have begun to monetise the concept of creating VIP experiences for attendees willing to pay a higher ticket fee. Facial recognition can improve that experience by recognising these individuals as they enter the venue, alerting employees to greet them by name, deliver their favourite snacks and beverages etc. On the other end, it can prevent access to known hooligans or overly-passionate fans who have caused trouble in the past.

Banking: Its accuracy makes facial recognition an ideal tool for identity verification in financial applications. The technology can replace a card scan at ATMs, helping to reduce fraud and skimming. There is even the potential to use it for ID validation for smartphone banking transactions, a fast-growing application for finance.

Healthcare: Early diagnosis by selfie is not science fiction – researchers with the National Human Genome Research Institute have successfully used facial recognition software to diagnose DiGeorge syndrome, a rare genetic disease. This early diagnosis can help healthcare providers deliver critical early interventions and improve their overall level of care. The same team of researchers is continuing to study diseases and other disorders to find additional opportunities for diagnosis via facial recognition. ■

Evaluate Biometric Authentication Pros And Cons, Implications

Hoping for a passwordless future? Multifactor authentication using biometrics may be the answer. Consider biometric authentication's pros, cons and implications before deploying.

By Jessica Groopman, Founding Partner of Kaleido Insights

As organisations and consumers around the world face an increasing number of cybersecurity risks, the search is on for more resilient security methods than traditional passwords. Recent studies have found stolen login credentials are the leading cause of data breaches. Around the globe, millions have suffered hacks and identity theft due to poor password hygiene, and most users have encountered a growing number of steps to log in to their digital services: Enter the code sent via text; answer a security question; take these steps before you can access this service.

These multiple factors are part of a broader trend to displace passwords with multifactor authentication (MFA). MFA requires users to present two or more pieces of evidence to an authentication mechanism. Evidence may include something they know, something they have, somewhere they are or something they are. Using multiple factors to authenticate can greatly reduce the risk of a hack.

Now, due to recent advancements in computing, increased quantities of data and decreased costs of hardware, a new authentication factor is going mainstream: biometrics.

The Rise Of Biometric MFA

Facial, fingerprint, iris, voice and countless other forms of biometrics are seeing widespread adoption and growth rates. Mobile giants have sold billions of smartphones with at least one form of biometric authentication baked in since 2012. Now, investment is spreading across sectors. Financial services, automotive, healthcare and education sectors are configuring biometric-based MFA to redefine access controls and safeguard assets. Before rushing to deployment,

however, security professionals must consider the pros and cons of biometric MFA and its broader effects.

Biometric Authentication Pros And Cons

The good news is that biometrics are extremely difficult to hack. This is because the variations are so unique or subtle that they require sophisticated tools, computation and distinctive data to replicate. For example, the voice has well over 100 parameters unique to each individual. Likewise, fingerprints would require some sort of physical interaction to replicate.

But the ironclad strength of biometric uniqueness has a chink in its armour: If bad actors compromise this data, it is impossible to recover or replace. Individuals cannot swap out their fingerprints or DNA like they can a password or credit card number.

Biometrics have significantly less friction than passwords and other traditional factors, such as PINs, keys or security questions. Instead of fumbling across media and devices—or scrambling to remember answers to obscure questions—biometric-based authentication simply requires presenting the biometric for scan. But with convenience comes additional risks. How could data, particularly sensitive biometric data, be used for purposes beyond access controls? How might multiple databases be combined for dragnets, for lucrative sale on the dark web or for other unintended consequences? What is the role of mass biometric-based authentication in societal surveillance?

Facial, fingerprint, iris, voice and countless other forms of biometrics are seeing widespread adoption and growth rates. Mobile giants have sold billions of smartphones with at least one form of biometric authentication baked in since 2012.

A third dynamic is the novelty of this technology at scale. Consider how biometric authentication has been around for decades in governmental and industrial security environments. These configurations ran on premises, often with physical tokens, and supported a small number of users. By contrast, AI-powered biometric authentication—such as voice recognition in financial services or facial recognition in airports—is designed to run at mass scale with diverse configurations, sometimes involving cloud service providers.

Whether the objective is convenience or scale, the risk of inaccurate recognition remains. Denial of entry due to erroneous scanning, data inaccuracy and compromise of the biometric—a cut finger, for instance—are several untested variables to running biometric authentication at scale.

What to consider when implementing biometric-based MFA

Based on these dynamics, here are some of the subsequent considerations for security professionals to keep in mind when implementing biometric authentication in MFA programs:

- Many factors are available for MFA. MFA includes a growing range of factors, including biometrics, PINs and encrypted tokens. When evaluating biometrics, understand criteria for the specific use case, existing security feasibility and potential financial implications.
- Biometrics require increased data and architecture security. In an age of corporate data breaches, companies must treat biometric data with heightened caution, which requires additional resources.
- Data minimisation is strategic. Security must lead cross-functional discussions and designs around limiting the collection and retention of data to that which is only relevant and necessary for a specific purpose.
- Distribute the risk. Avoid centralised honeypots of sensitive biometric data. Prioritise distributed processing with minimal functionality over centralised processing with multiple functions.
- Friction has benefits. Increased safeguards often require more steps in UX, but avoiding friction at all costs can put users at greater risk.
- Educate and engage users. Lean into the opportunity to educate, involve and listen to users during deployment. Use this collaboration to forge trust and improve UX.

Although the technology remains in relative infancy in terms of commercial application, biometric authentication modalities introduce employees and consumers to a fundamentally new interface. As sensor and software technologies continue to evolve into mainstream infrastructure, employees' physical selves may become key agents in digital services and transactions. ■

RFID For Indoor Asset Tracking

RFID technology isn't a standalone solution for indoor positioning. As part of a multi-technology system, however, it can be highly effective.

Reproduced from IoT For All

The venerable RFID tag traces its ancestry to the "friend or foe" transponder systems developed for military aircraft beginning in WWII. Since then, RFID has earned its place as a reliable asset identification system. Recently, it has been marketed as a solution for real-time indoor positioning. This post provides a brief overview of how RFID works, how it might be used for indoor asset tracking, and how it compares to alternatives.

How RFID works

An RFID system—RFID stands for "radio-frequency-identification"—comprises two components: a transponder (or tag) containing data that can be read over RF and an interrogator (or reader) that can read the transponder's data. The specific way in which these components communicate (known as their "coupling mechanism") determines the range, complexity, and cost of the system. ("Coupling" in this context refers to an energy transfer between tag and reader.) Currently, three types of coupling mechanisms compete in the market: inductive, capacitive, and backscatter.

Inductive Coupling

Inductive coupling has been present since the early days of RFID when the systems involved bulky tags with complicated antenna mechanisms used to track large objects (e.g., cars, cattle). The inductively coupled tag draws energy from the magnetic field created by the reader and modulates it. The reader measures the perturbation by

the tag and decodes it as data. The magnetic fields used in these systems drops off rapidly, affording inductive coupling an effective range of about 1cm to 1m.

Capacitive Coupling

Capacitive coupling systems were created to lower the cost and size of RFID when large inductive systems were the only option on the market. They employ conductive patches on both reader and tag to form a capacitor and signal data by varying the capacitance of the circuit. These systems are extremely close range—1cm—and the orientation of the patches matters, so a typical application would be an ID card that must be inserted into a reader. As inductive circuits shrank, so too did the market for the more limited capacitive systems. Indeed, most RFID systems today use some version of inductive coupling. They are, however, still limited by magnetic fields' rapid drop in strength at a distance. To reliably achieve longer range, RFID systems must use higher frequency signals and rely on the electric side of the electromagnetic signal.

Backscatter Coupling

Backscatter coupling employs a reader that sends out a UHF or microwave signal that impinges on a tag and then reads patterns in the reflected energy. Whether the increased range is an advantage or disadvantage depends, of course, on the use case. Scanning pallets as they pass through a large warehouse gate? Great. Unlocking doors or disseminating payment information? Probably less desirable.

Types of RFID Tags

The RFID market delineates systems according to how RFID tags are powered. Whether a tag has onboard power available affects its size, price, read range, and whether it can support additional sensors.

Passive Tags

Passive tags have no internal power source. They work by siphoning some of the power in the interrogator's signal to modulate their response. This allows them to be cheap, durable, and quiet (in the radio spectrum). Lacking consistent energy, they can't contain volatile memory, meaning they can't be used to write and store sensor data. They have a lower range than powered alternatives and require high power, high-cost readers.

Semi-passive Tags

Semi-passive tags (also known as "semi-active" and "battery-assisted" tags) have an onboard battery. Like passive tags, they only transmit in the presence of a reader's signal. The battery can power a sensor as well as the antenna. A powered antenna allows more signal to reflect back to the reader, which provides a longer range than wholly passive tags. They are bulkier and more expensive than passive tags and have a battery-limited lifespan.

Before assessing RFID's merits as an asset tracking technology, we need to clarify what we mean by "tracking". RFID has, since its inception, been used to track assets in a sort of spreadsheet sense. It makes it simple to identify and log which tracked items are nearby. If your goal is to make sure all of the train cars that went through gate A also made it through gate B, or whether an employee swiped into a building, then RFID is a well-tested, proven solution.

Active Tags

Active tags have a local power source (e.g., battery, photovoltaics) and broadcast their own signal. Despite their marketing label, these are not technically RFID devices since they don't depend on receiving and modulating a reader's signal. Instead, they're short range radios. From an operations perspective, this distinction is likely not all that important, so we follow the market and include them here. Compared to passive and semi-passive tags, active tags have significantly greater range (up to 1km) as well as increased memory capacity, size, and cost, and they can work with weaker readers.

Tracking Assets with RFID

Before assessing RFID's merits as an asset tracking technology, we need to clarify what we mean by "tracking". RFID has, since its inception, been used to track assets in a sort of spreadsheet sense. It makes it simple to identify and log which tracked items are nearby. If your goal is to make sure all of the train cars that went through gate A also made it through gate B, or whether an employee swiped into a building, then RFID is a well-tested, proven solution.

In such use cases, RFID competes most directly with barcodes or QR codes. It offers the obvious advantage of being readable at a distance. Active or semi-active RFID

tags can provide valuable sensor information. On the other hand, passive readers are very expensive, and powered tags are costly and have a limited lifespan.

A more challenging type of tracking is knowing the (nearly) real-time location of a tracked asset. Although this is a relatively recent use case for RFID, there are already quite a few commercial solutions on the market.

The way these systems work varies. Some systems use RFID purely for object identification while leveraging another technology for ranging. Those that rely purely on RFID almost exclusively use active RFID tags. There is some exciting research that uses passive RFID tags, but the cost of passive readers and the low range of these systems makes them commercially prohibitive. Real-time location systems (RTLS) that use active RFID tags behave similarly to competing technologies—Bluetooth, Bluetooth Low-Energy (BLE), Wi-Fi, Ultrasonic, and Ultra-Wideband (UWB). The RFID versions are largely based on the LANDMARC system, which determines location by comparing the Received Signal Strength (RSS) of an active tag's signals with the RSS of reference tags with a known location.

Active RFID has a much greater range than BLE. It's capable of spanning a kilometre in open air compared to BLE's ~70m. This is less important in indoor environments with obstructions (e.g. walls or floors), but in warehouses or barns active RFID's range might allow businesses to make do with fewer readers, cutting costs and reducing potential failure points.

A Problem (Bleed-Through) and a Solution (Hybrid Systems)

RFID has a few drawbacks as a tracking solution. Like all RF / RSSI based solutions, it suffers from bleed-through. Since RF signals can penetrate walls, it becomes difficult to determine from which room a tag is transmitting. The high bandwidths used by active trackers—especially long range trackers—is highly subject to interference. And, compared to BLE, both the tags and the readers are very expensive. RFID finds its greatest success as part of a hybrid system. It provides reliable identification, which can supplement systems that rely on ultrasonic, infrared, or ultra-wideband for location information.

Currently, RFID technology is not ready to provide a standalone solution for indoor positioning. It is not alone in that respect. As part of a multi-technology system, however, RFID brings to indoor positioning its decades-long history of reliable identification. ■

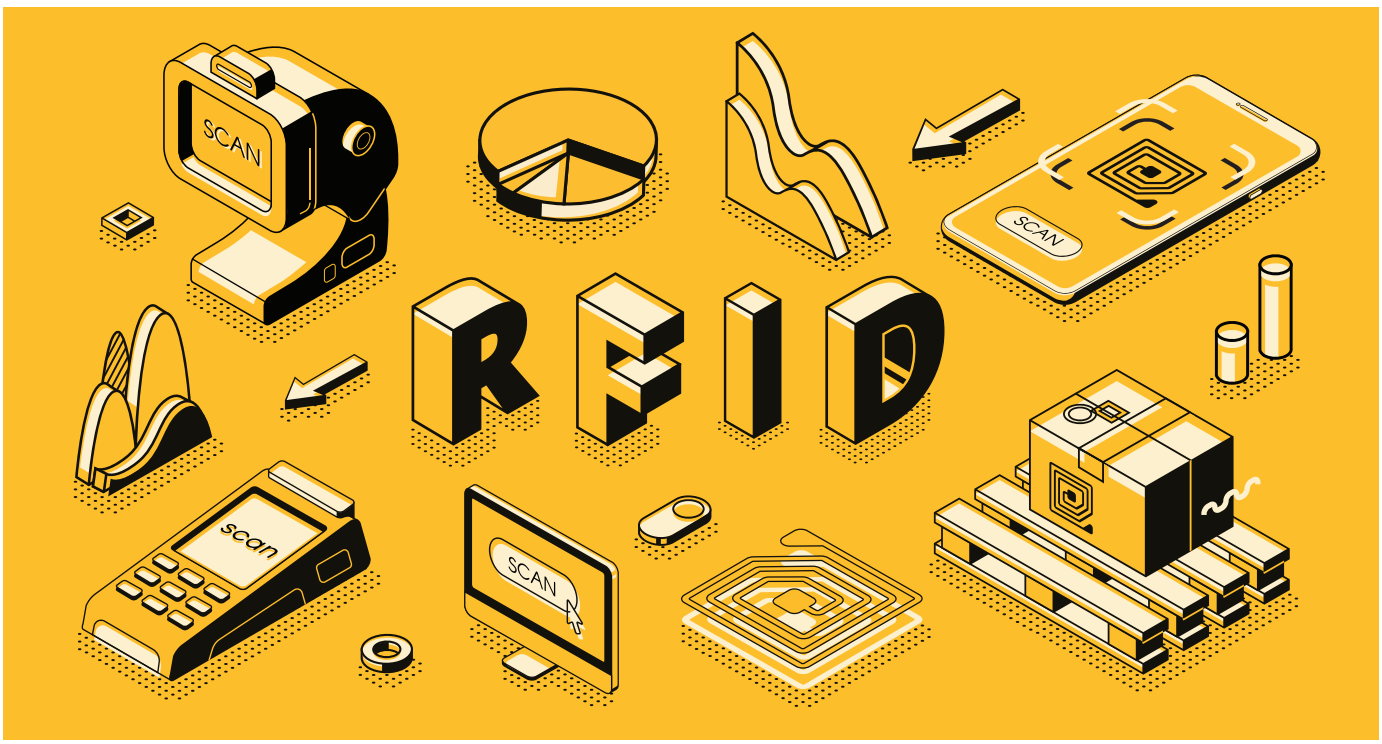
Smart Cold Chain: How IIot And RFID Save Products From Spoilage

Technologies such as RFID and IIoT can help to address cold chain inefficiencies by providing increased visibility into the locations, properties, and conditions of sensitive products.

By Boris Shiklo, CTO at ScienceSoft

Since the supply chain deals with sensitive products, such as food, medicines, and modern nanomaterials, even a minor mistake, be it improper temperature control or higher-than-recommended humidity levels, can lead to product spoilage. In the pharma industry, 20 percent of medicine is damaged due to shattered cold chain processes. Food waste is even worse. According to BCG, in the US alone, 1.6 billion tons of food spoils every year due to cold chain malfunctions.

In this article, we'll explore how RFID and the Industrial Internet of Things (IIoT) technologies can help to address cold chain issues and make cold chains more reliable and transparent.



RFID and IIoT: Their Role And Working Principles

Major cold chain inefficiencies are frequently traced back to enterprises not having enough visibility into the location and condition of their sensitive cargo. RFID and IIoT provide access to data and thus eliminate the root cause of cold chain issues. Here is a closer look into how the technologies work.

RFID

Typically, there are three main components in an RFID system: RFID tags, RFID antennas, and RFID readers.

In the cold chain, predominantly passive RFID tags are used; they're smaller, cheaper, and more mobile. These tags do not have a power supply and should be powered by the energy from RFID readers to transmit data.

RFID antennas (typically integrated with the RFID readers) supply the energy for the tags and forward the data from the tags back to the readers.

RFID readers are used to read the data from the tags. A reader takes in a radio signal from RFID tags, converts it into digital information, and sends it to the cloud platform for further processing (together with the data about the location of the reader and the time of the reading). This is where IIoT takes over.

IIoT

IIoT uses a network of connected sensors attached to product packages, warehouse shelves, and vehicles to track the conditions in which sensitive products are stored. Along with it, the cloud platform—the core of an IIoT system—provides storage and analytics capabilities for both RFID- and sensor-generated data. The IIoT system takes in RFID and sensor readings, runs them through analytics algorithms, and visualises the findings in the form of dashboards, reports, real-time product location maps, etc. In addition, IIoT systems use web or mobile applications to enable communication with users, for example, to alert warehouse staff if the temperature at a warehouse approaches a critical threshold.

RFID And IIoT: The Parameters to Track

RFID and IIoT help to maintain product quality at all cold chain segments and provide the opportunities to monitor the following:

- **Product Locations And Movements**
RFID is used to track sensitive products at manufacturing and storage facilities and to establish when the cargo leaves or arrives at a particular facility. Whenever RFID-labelled products pass RFID readers installed at the key points of a factory or a warehouse, the tags are automatically scanned and located, and the locations of the corresponding products are automatically updated in the database.

To create an even more coherent tracking network across the cold chain, RFID can be paired with GPS. GPS can keep track of vehicles transporting cargo, establish where a particular vehicle is in its delivery cycle, and estimate when it's likely to get to a destination point. Also, when a manufacturer outsources logistics operations, a logistics company can collect GPS data from vehicles involved in the transportation of products and share it with the manufacturer.

- **Properties Of Individual Product Packages**
With RFID and IIoT in place, inventory specialists can drill down any parameter to get a well-rounded view of the products on hand. They can learn, for instance, that out of 1,000 packages of SKU X, 200 have less than 30 days till expiration. Now, when an inventory specialist receives an order for SKU X, they can choose the packages with the closest expiration date and ship them first.

- **Product Storage Conditions**
To preserve the quality of sensitive cargo, temperature and humidity sensors can be attached to the warehouse shelves or the inner sides of refrigeration units in which products are stored and transported. As a result, the manufacturers get access to up-to-the-second information about the ambient parameters affecting the shelf life of sensitive products.

To create an even more coherent tracking network across the cold chain, RFID can be paired with GPS. GPS can keep track of vehicles transporting cargo, establish where a particular vehicle is in its delivery cycle, and estimate when it's likely to get to a destination point. Also, when a manufacturer outsources logistics operations, a logistics company can collect GPS data from vehicles involved in the transportation of products and share it with the manufacturer.

A Case In Point

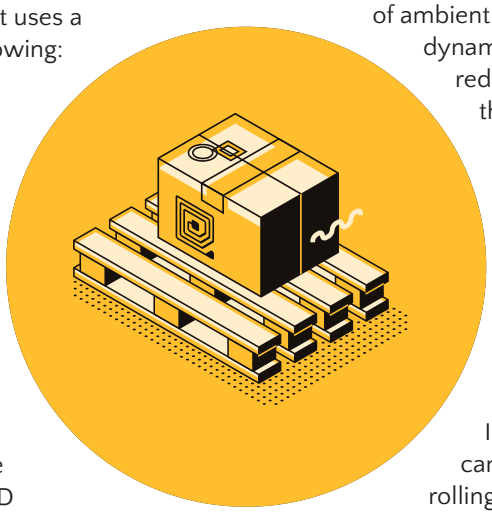
Let's consider the example of how RFID and IIoT can be applied for optimising cold chain operations in the dairy industry.

Warehouse workers pick the packages and transport them to the shipping area of the warehouse. At the exits of the shipping area, RFID readers scan the RFID tags attached to the packages and check if all the requested packages are being shipped. Due to the integration of an IIoT solution with an order management system, the shipping is automatically recorded upon scanning.

Say a dairy enterprise has a new batch of brie cheese manufactured. The cartons of cheese are packaged with each package getting an RFID tag. The tags' IDs are correlated with the data about the packages they are attached to (the number of cartons in the package, the date of production, the location in the warehouse, etc.) and saved to a cloud database.

When the enterprise receives a new order for, say, 1,000 cartons of cheese, an inventory specialist uses a web or mobile application to do the following:

- Check if the required number of cartons is available.
- Check which packages have less time till expiry, so they can be sent to distributors first.
- Quickly locate the required packages in a warehouse (row, shelf, etc.).



Warehouse workers pick the packages and transport them to the shipping area of the warehouse. At the exits of the shipping area, RFID readers scan the RFID tags attached to the packages and check if all the requested packages are being shipped. Due to the integration of an IIoT solution with an order management system, the shipping is automatically recorded upon scanning.

The packages are put in vehicles, and each vehicle is equipped with a temperature and humidity sensor. The sensors provide data about the condition of the cheese en route, notify drivers of the need to adjust the ambient parameters, and inform the driver and the manufacturer whenever transportation conditions are violated. On the way, a vehicle's GPS tracker updates the manufacturer and distributor about the location of the vehicle involved in the delivery, so they can dynamically track the status of the shipment.

The Benefits Of The Connected Cold Chain

The data obtained through RFID and IIoT makes cold chains more streamline and drives the following improvements:

- **Waste Prevention**

Forty percent of all perishable products never make it to the customers, which is a large amount of waste. Provided with detailed, real-time information about the storing and shipping conditions of sensitive cargo, manufacturers can take preventative measures to save the products and to reduce waste considerably.

- **Optimised Inventory Management**

The more detailed data there is available to inventory specialists about product locations and properties, the more likely they are to have the right products at the right time in the right place. As a result, they can lower the amount of perishable cargo on hand, still being able to meet customer demand at the end of the cold chain.

- **Lower Operational Costs And Better Customer Service**

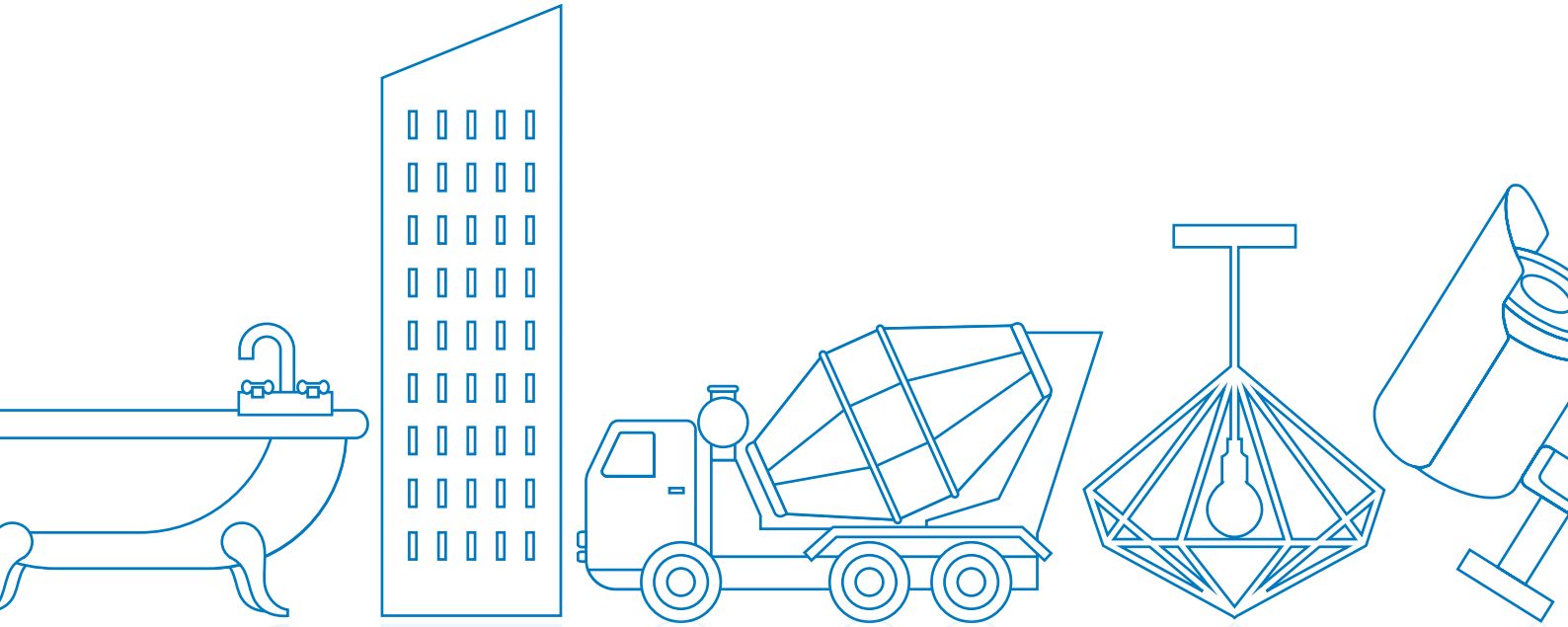
The application of RFID and IIoT in the cold chain makes inventory management more comprehensive. Receiving timely alerts about shipping delays and the violation of ambient parameters, manufacturers can dynamically manage cold chain issues to reduce operational costs and to increase the quality of customer service.

Things To Keep In Mind

Nothing as massive as the connected cold chain comes without challenges. Resorting to technology-driven solutions, enterprises should keep in mind the following points:

Implementing a connected cold chain can be time- and effort-intensive, and rolling out the technological infrastructure required for the connected supply chain implementation usually involves substantial investments. Therefore, the cost of products to track or the cold chain optimisation potential should be high enough for the solution to pay off.

Some RFID tags may encounter collisions when scanned simultaneously. So, enterprises should carefully consider the conditions the tags will be used in to choose the tags of optimal frequency, and deploy RFID readers with an appropriate coverage and reading rate. ■



bathroom + kitchen today

SEAB
SOUTHEAST ASIA BUILDING

lighting today

SOUTHEAST·ASIA CONSTRUCTION

SECURITY SOLUTIONS TODAY

We reach out to various segments of the professional readers within the building, construction, security and lighting industries across Asia-Pacific region with our specialised publications in print and digital formats as well as on social media platforms.

Visit our website **www.tradelinkmedia.biz** for more information.

Scan to visit our website

TRADE LINK MEDIA PTE LTD

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

Biometric IoT Sensors Shape The Future Of User Interfaces

Biometric interfaces unlock new capabilities and risks with IoT sensors, including security based on human features or virtual assistants tailored to recognise voices.

By Jessica Groopman, Founding Partner at Kaleido Insights

Biometric IoT sensors introduce new interfaces and capabilities for devices but also present implications for IoT builders and suppliers to consider.

An interface is defined as a shared boundary or point of interaction between humans and technology. For decades, screens have dominated how people think about interacting with technology. The last decade brought about a sea of change in interfaces, with the rise of mobile radically shifting how people interact with one another, businesses and objects all around. Sensors, cloud computing and networked infrastructure powered this shift and redefined entire industries, such as taxis and the media; brand experiences, including ordering coffee or turning on the lights; and business itself, such as remote management and enterprise security.

The next decade will de-emphasise screens, as the human body becomes the predominant interface for technology. Biometric interfaces have been around for decades, but recent advancements in sensors, software and big data processing now power significant growth, a 22.9% compound annual growth rate, according to Tractica's report "Global Biometrics Market Revenue to Reach $15.1 Billion by 2025." In particular, the convergence of AI with IoT powers unstructured data processing at scale and creates new uses across sectors.

Biometric Data Promotes New Uses And Partnership Opportunities

Certain biometrics lend themselves to uses that traditional IoT devices did not support, including biometric authentication, user-specific commands and health monitoring. For example, an electronically recorded voiceprint offers a uniquely identifiable representation of an individual, akin to a fingerprint. Speech recognition alters the interface of search or device commands and serves as speaker recognition.

Voiceprints create opportunities for multi-tenant or multiuser personalisation in smart home or industrial control experiences, but also a host of new uses across sectors, including payment from devices, pharmaceutical dispensing

Each biometric IoT sensor introduces new considerations for sensor arrays. The use of heart rate variability sensing measures the time interval between heartbeats and is affected by age, health status and range of mental, physical and emotional experiences.

or adherence, automotive access controls, public safety and security, health and wellness monitoring, recycling, second-hand use and security.

New capabilities complement the drive toward ecosystem-based business models, as partnerships support improved user experiences, service marketplaces and novel monetisation opportunities.

Biometric Data Introduces New Risks

Biometric data also introduces new risks that are absent from nonbiometric product engagement or performance metrics. For example, using biometric IoT devices:

- May be subject to existing regulations, such as the Biometric Information Privacy Act or Children's Online Privacy Protection Act.
- May incur greater harm or sanction in the event of misuse or abuse.
- May involve more intimate and sensitive data, such as a medical condition or learning disorder.
- Carries a higher risk of breach because health data is more highly valued on the dark web market.
- Carries irrevocable risks, such as identity theft of DNA, versus revocable risk such as replacing a password.

Adding to the complexity, IoT builders may not be aware of biometric-specific risks, liabilities or downstream effects. This underscores the need for multidisciplinary collaboration on IoT product and business model design, as well as data security and lifecycle management.

Biometric Data As Triangulated Data In The Quest For Context

IoT builders must also evaluate the opportunities and risks in the context of triangulating, fusing and inferencing multiple data sources together. This common practice compounds the value of data by driving more contextual product experiences or altogether new services. For example, Amazon's Alexa applies multiple data sources to automatically learn individuals' voices to adjust its functionality. Alexa applies speaker recognition to give specific permissions or skills based on the user's age.

Each biometric IoT sensor introduces new considerations for sensor arrays.

The use of heart rate variability sensing measures the time interval between heartbeats and is affected by age, health status and range of mental, physical and emotional experiences. Imagine the contextual experiences possible when combining heart rate variability data with diet, sleep, movement and social interactions. Imagine further, the benefits to caretakers, elderly, parents or athletes.

Manufacturers and IoT designers are confronted with new design questions, such as:

- What are the parameters for using a biometric sensor for each use?
- What new uses are possible?
- What are the accuracy thresholds and risks of machine error?
- How will the data be applied to achieve customer outcomes?
- How might the data support services to under-serviced markets?
- How might data be misused, whether inadvertently or nefariously?

Awareness Is More Important Than Ever

New interfaces always disrupt traditional industries and models, but biometric IoT interfaces merit renewed attention and communication with consumers and employees. People will no longer read screens, but the screens will read them – not only interactions and behaviours, but bodies and physical and emotional reactions, both conscious and even subconscious. Biometric data can be applied to diverse consumer products, improved security and wellbeing, but they also place undue risk to consumers and businesses alike. Now, more than ever, IoT providers have a unique opportunity, not only to streamline UX with biometrics, but foster renewed human trust through humane designs. ■

IAM-driven Biometrics In Security Requires Adjustments

IAM is foundational to cybersecurity, but the latest systems use biometrics and other personal data. Learn how to cope with the resulting compliance and privacy issues.

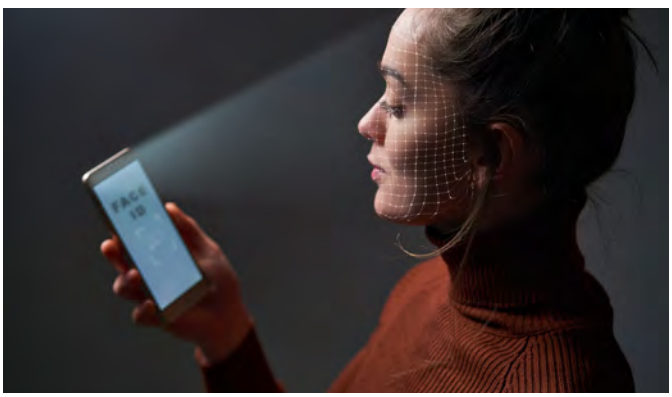
By Mary K. Pratt, TechTarget

When security executive Chris Dimitriadis sought to strengthen his team's cybersecurity profile, he added biometric elements to its identity and access management program.

Employees who need access to the most sensitive data – whom Dimitriadis labelled "privileged users" – must use either their fingerprints or facial recognition scans to open applications that hold that information.

The use of biometrics in security systems simplified the company's identity and access management (IAM) program while at the same time strengthening it, according to Dimitriadis, who is responsible for IT services for customers of Intralot, a Greece-based lottery vendor and operator, and a board member and prior chairman of the IT governance association ISACA.

"The simpler the authentication is for a human, the better security it is at the end of the day," he said. "That's why I favour biometrics; it's easier, and it's also very user-friendly. The more we help humans, the easier security becomes, the better compliance you have."



There are, however, additional considerations and trade-offs that come with such IAM programs and technologies, Dimitriadis and other security experts acknowledged.

IAM systems are increasingly asking users for more personal information that organisations must then ensure is secure, well managed and compliant with data privacy regulations and user expectations.

Employees who need access to the most sensitive data – whom Dimitriadis labelled "privileged users" – must use either their fingerprints or facial recognition scans to open applications that hold that information.

IAM Deployments And Biometrics In Security

Although organisations generally consider IAM to be a foundational part of cybersecurity best practices, many still struggle with implementing and maintaining an effective identity and access management program. Findings from the 2018 "Assessment of Identity and Access Management" study conducted by Dimensional Research for IAM provider One Identity, highlighted some of the limits and challenges that come with IAM.

For example, only 15% of the 1,000-plus responding IT security professionals said they were completely confident that their organisation would not be hacked because of an issue with its access control program. On the other hand, 19% said they weren't confident that such a hack would not happen, while 66% said they were only fairly confident such a hack wouldn't happen.

Such statistics help explain why security experts see organisations increasingly adopting more robust IAM practices, such as two-factor authentication, physical biometrics and behavioural biometrics.

Passwords are also cumbersome and often less effective than biometrics and behaviour-based analytics, so "people are trying to get rid of the passwords, and rightly so," said George Moraetes, a security consultant and CISO with his firm Securityminders.

Maturing Programs And Their Security Challenges

But security, privacy and security executives are finding that the move beyond single sign-on passwords comes with its own security and privacy challenges. These biometrics capabilities, behaviour-based security analytics and other advanced IAM systems ask users to provide data that organisations must now safeguard. Simply employing biometrics in security can create security headaches.

"It would be ironic if you're collecting this kind of data to secure your systems and then that data is left vulnerable for unauthorised access," said Rita S. Heimes, general counsel and data protection officer with the International Association of Privacy Professionals.

Additionally, organisations are seeing some people push back against having to use deeply personal information, such as one's own fingerprints, just to do their jobs.

Steve Wilson, an analyst with Constellation Research, pointed to an Australian legal battle involving an employee

who was fired after refusing to provide his fingerprints to his employer, as required for a new security scanning system. The country's Fair Work Commission found the employer unfairly dismissed the employee.

"He won his unfair dismissal case on the grounds that he wasn't given any reasonable alternative to biometrics and was therefore not being accorded due-consent processes," Wilson said. "'Consent' isn't consent if you are forced to use the system."

Wilson and others said business leaders will need to address such issues as they implement biometrics in IAM systems. They'll also have to ensure the personal information that's collected and stored -- whether it's fingerprints or behavioural patterns – is done so in ways that are secure and meet all regulatory requirements, such as the European Union's General Data Protection Regulation, or GDPR.

Employees who need access to the most sensitive data – whom Dimitriadis labelled "privileged users" – must use either their fingerprints or facial recognition scans to open applications that hold that information.

Steps For Using Biometrics In Security

Organisations need to consider how biometrics and other advanced IAM practices fit into their overall security program and to think of access control and data protection holistically, experts said. Organisations must understand what data they have, what data they really need, how to get rid of what they don't require, where data is stored and how it's stored.

Heimes stressed that organisations should only collect and keep what they need in order to get their work done. Dimitriadis agreed, saying: "Know where your data sets are, how you classify them, how important each data set is and then ... decide whom to give access to it. It may sound like a simple task, but it turns out to be very, very complex."

That analysis should inform the controls required, with business leaders determining what level of data sensitivity warrants the use of sophisticated IAM systems, such as those that are biometrics-based.

Wilson said organisations should ask the following: Is biometric security a proportionate response to the security problems a company is trying to solve? Is the biometric really going to be as effective as they think? Is it creating new risks by accumulating biometric data? How are the biometric scans and reference templates being stored?

Jason Taule, vice president of standards and CISO for HITRUST, said he advises organisations to start by considering the level of risk, and whether two-factor authentication or other non-biometric options available address access requirements.

From there, they should invest in identity vetting, determining how they'll validate that someone is who they purport to be.

They also need to evaluate their IAM vendors to determine how they treat the personal information they use to grant access, he said. He noted that some vendors collect and store the fingerprint, facial or other personal information they use to authenticate users. Others may not store that information but only access it once, assign values derived from it and then store those values.

Although storing only numeric values greatly lowers the security risk, organisations should still vet those vendors to ensure they follow strong security protocols in addition to maintain their own enterprise security policies and procedures.

Organisations should also vet the functionality of the system. "You also want strong reporting and integration with your existing infrastructure," he added. Experts also advise full transparency when it comes to implementing biometrics in security processes.

"The employee has to be fully aware on why they're being asked to provide biometrics, the employee should know in advance where and why it's happening," Moraetes said. ■

3 Ways Automated Backup Can Aid Your Data Protection

Automated backup can help you meet all-important recovery point objectives. Take advantage of automation in the backup process, as it can improve your recovery down the line.

By Paul Kirvan, TechTarget

Backing up data and other information assets is one of the most important activities an IT department performs, and it should also be a priority among senior management. One of the top considerations is how often your organisation backs up data and other information resources.

You should try to back up as often as possible. Naturally, given the typical IT department's daily list of activities, data backups might be a secondary activity. Compared to launching a new system, reconfiguring network elements or evaluating new products and services, backups might not occur unless the organisation has established a data backup process and team.

Automated backup, in which the backup engine is programmed to perform specific activities at designated times, can address that challenge. When performing backups, especially those with a significant frequency – such as hourly backups – the organisation should consider such elements as network bandwidth and processing overhead.

If the backups move to an on-site repository, such as solid-state disk, RAID or NAS, bandwidth might not present much of an issue, especially if your organisation designates dedicated network resources exclusively for backups. By contrast, off-site backups to alternate data centers, other offices or external third-party managed data backup resources might have bandwidth limitations based on backup frequency.

Streamline Your Backup With Automation

Automated backup should factor in these considerations so that the organisation can initiate a "set it and forget it" arrangement. This is the first benefit of automated backups: simplifying the backup process through automated scheduling.

A second benefit of automated backup is addressing a file loss situation. Assuming your organisation regularly performs backups, the chances of lost data having been backed up improves with automated backups. While there's no substitution to backing up work files as often as possible – and many applications can also perform automated backup – the likelihood of losing in-use files and data still exists. Automated backups can help reduce the likelihood of an "oops" moment.

Regularly scheduled backups of active files, databases, virtual machines and other applications can improve disaster recovery and, by extension, business continuity – a third benefit to automated backups. Whether on-site or remotely stored, availability of regularly backed up files and systems increases the likelihood of an organisation's successful recovery from a system outage or a malware attack.

For many organisations, the recovery point objective (RPO) presents an additional important metric. A lower RPO value means your organisation must back up data more frequently. Automated backup can help ensure that you maintain RPOs agreed to by management.

Automation benefits many data management applications. Although you can still manually initiate backups, availability of automation to streamline the backup function delivers important benefits to organisations. ■

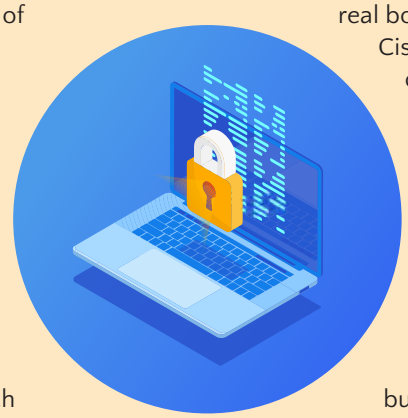
Data Privacy Benefits Outweigh Spend, Says Cisco

Cisco's 2020 data privacy study shows organisations can generate substantial returns on their data privacy and protection spending.

By Alex Scroxton, ComputerWeekly.com

The benefits of spending on data privacy and protection average 2.7 times the original investment – 3.5 times in the UK – with 77% of buyers saying they have received "significant business benefits" from privacy, beyond merely compliance, according to Cisco's 2020 Data privacy benchmark study.

This means that that for every dollar of privacy spend, global organisations are getting $2.70 of benefit, while British organisations are getting $3.50 worth of benefit. Nearly half of businesses saw a greater than twofold return, 33% were breaking even, and 8% were getting back less.



This is the third edition of Cisco's now annual research paper, which looks at corporate data privacy practices worldwide, and this year shows significant growth in benefits for those that adopt strong privacy practices 18 months after the introduction of the European Union's General Data Protection Regulation (GDPR), which unsurprisingly seems to have been a catalyst for privacy investment.

Based on a double-blind survey of 2,800 security professionals, the report shows how customer demands for increased protection, the threat of data breaches and misuse by insiders and threat actors, have also spurred organisations to plough cash into privacy.

"With this study, we now have empirical evidence of privacy investments paying off for companies – particularly with improved customer relationships, revenue impact and real bottom-line results," said Cisco vice-president and chief privacy officer Harvey Jang.

Cisco noted that the return on investment (ROI) benefits appeared to be fairly similar regardless of organisational size. Although larger businesses are quantifiably spending more money and getting more benefits, the ratio of benefits to spending is persistent across large, mid-size and small businesses.

Besides growing RoI – over 40% saw benefits at least two times that of their spend – investment in data privacy also generates operational and competitive advantages, said Cisco.

Over 70% of organisations – up from 40% in 2019 – now say they are now more agile, have a better competitive advantage over rivals, are more attractive to investors, and are better trusted by customers.

A higher degree of accountability was also found to translate to increased benefits, with those that had higher accountability scores – as per the Centre for Information Policy Leadership's Accountability Wheel, a framework for managing and assessing organisational maturity – were spending less on rectifying breaches that did occur and experiencing fewer delays in their sales cycles.

Reflecting tighter worldwide regulations, 82% of respondents to the study said they now saw privacy certifications – such as ISO 27701, the EU/Swiss-US Privacy Shield and APEC Cross Border Privacy Rules – as a buying factor. Respondents in India and Brazil seemed most likely to agree external certifications are now important in their buying decisions.

Cisco provided a short checklist of steps organisations can take to improve their data privacy posture. These include: improving transparency about processing activities, and being upfront and clear about what you are doing with user data, and why; obtaining external certifications, as above; going beyond the legal bare minimum; and building strong internal governance and accountability to demonstrate to stakeholders that your privacy programme is mature. □

How Privacy Compliance Rules Will Affect IT Security

As companies scramble to comply with consumer data privacy compliance mandates, like GDPR, CCPA and others on the horizon, IT security will shoulder much of the process burden.

By Ben Cole, TechTarget

With companies around the world just getting used to GDPR, those doing business in California must now prep to comply with the state's CCPA, and more consumer privacy regulations are on the horizon.

Companies required to follow these privacy compliance mandates are under pressure to make extensive changes to their IT and security processes – and quickly.

"There is a big need to have a clear plan in place for personal data—not only how it is being used, but how it is distributed," said Derrick A. Butts, chief information and cybersecurity officer of IT at Truth Initiative. "More transparency is needed as far as how companies are doing business because they are going to be held accountable."

Experts agree that privacy compliance rules, like the EU's GDPR and the California Consumer Privacy Act (CCPA), are certainly needed as consumer data continues to be a target for hackers. But privacy mandates leave companies scrambling as they add staff, update processes and implement tech like AI to maintain compliance.

These efforts could prove costly: An independent economic impact assessment prepared for the California attorney general's office found the CCPA could cost companies a total of up to $55 billion in initial compliance costs.

Authorising A 'Verifiable Consumer Request'

The new consumer privacy rights under CCPA alone will require many companies to implement policies and procedures to comply. One such rule is the verifiable consumer request

requirement that enables California consumers to request access to their personal information and ask that it be deleted. Upon receiving such a request, the covered business must verify the identity of the requesting individual and respond.

Businesses must establish practices to verify the identities of requesters or risk providing unauthorised, fraudulent third parties access to personal information. This burden will likely fall on the security department, said Scott Giordano, vice president and senior counsel of privacy and compliance at Spirion LLC, during a session titled "What the California Consumer Privacy Act Means for Your Security Program" at the 2019 (ISC)2 Security Congress in Orlando, Fla.

"You have to verify that person is who they say they are," Giordano said. "Who are the lucky folks likely to get that job at your company? It's not going to legal—legal is going to IT. Then, IT calls IT security."

Handling these types of requests will likely become a subindustry in and of itself down the road, Giordano said, but until then, the organisation is responsible to make sure the verification process is secure.

"More transparency is needed as far as how companies are doing business because they are going to be held accountable."

To make this job at least a little easier, Giordano said, steps like creating a data inventory, establishing processes to get consumers their information under deadline and making updates to the organisation's privacy statement can help.

"The onus is going to be on you guys to establish security controls for everything now for CCPA," Giordano told the audience at the (ISC)2 conference. "It's going to be a huge effort."

Designing Solutions With The Right To Privacy In Mind

One big obstacle is that, in the past, most of the engineering for new tech focused on gathering as much information as possible and then building a business model around it, said Alan Conboy, office of the CTO at Scale Computing.

This creates a huge burden on companies that built an entire business model on data collection, data mining and sharing data. Privacy compliance rules force them to try to track down exactly what data they have and then establish processes to isolate certain data to comply with mandates.

"They haven't focused on that capability, historically, at all," Conboy said.

This will leave many companies understaffed and unprepared to implement intricate data protection and security requirements to comply, he added.

"If admins are already struggling today with just subcomponent pieces, then that tells me there is way too much complexity already involved in their day to day," Conboy said. "These regulations add to that complexity exponentially."

As a result, more companies are turning to technology, such as AI and machine learning, to automate at least some regulatory compliance processes, such as data location or extraction. Old-school techniques, such as retention schedules, can help as well, said Ripcord Inc. CEO and founder Alex Fielding.

But, while Fielding said retention schedules in the past were sort of "loosey-goosey," privacy compliance rules increase the risk of exposure dramatically when data is kept beyond the expiration date.

"You could be sitting on a giant corpus of information that contains [personally identifiable information], and you may not even know it if you don't have the tools to track it," Fielding said.

Fielding added that many companies have good intentions about protecting consumer privacy but, in the past, have lacked the tools to do it. The compliance mandates force companies to act faster about implementing data privacy protection, he said.

Plus, privacy compliance is not optional anymore, and substantial fines and penalties for noncompliance will also help change behaviours, experts said.

"The days that companies could take their customers data for granted and not worry about the privacy implications for the consumer or the security implications for the company are totally over," Fielding said. ■

Protect Against Evolving Data Security Threats

As data security threats evolve, knowing how to protect your data is more important than ever. Learn about the latest security threats and how to ward them off.

By Kevin Tolly, Founder of The Tolly Group

Corporate data needs to be secure, private and protected. That's obvious advice, but the steps organisations should take to prevent data security threats and keep their data safe from hackers are much less apparent.

This article looks at some of the tactics—both old and new—hackers are using in their attempts to access your data. Spoiler alert: Protecting your organisation from data security threats requires a comprehensive approach.

Security isn't just orchestrated through a single security department, and it can't merely reside in a single layer of a protocol stack. Threats come from various sources, from both inside and outside an organisation. Combating these threats requires a multilevel and multifaceted strategy that includes not just IT, but other departments, including HR, accounting and legal. Here's a look at some trends that pose the biggest threats to corporate data and the actions you can take to protect it.

Undetected Data Security Threats

These can be called exploits waiting to happen. Vulnerabilities that may already exist in your corporate systems can be used to compromise data privacy. For example, legacy systems might have built-in backdoor administrative passwords. These potential superuser identities might have access to all data, thus enabling the users to steal data without even having to hack a real user's credentials.

Protecting your data means making a list of all third-party and in-house IT systems in use. Verify whether these systems have any superuser IDs. If so, confirm that the user ID's password isn't set to the system default and that it is either disabled, if not needed, or, if used, guarded by a strong password.

effectively open a backdoor that can be used to compromise data—even from within the corporate network. ACLs created for special groups or projects that are no longer active should be deleted.

Self-inflicted Attacks

Despite an organisation's best efforts, many breaches are essentially self-inflicted: Phishing attacks, propagated through emails cloaked with the look and feel of legitimate senders, are a major hazard today and likely will continue to be so in the years to come. These attacks become

Protecting your data means making a list of all third-party and in-house IT systems in use. Verify whether these systems have any superuser IDs. If so, confirm that the user ID's password isn't set to the system default and that it is either disabled, if not needed, or, if used, guarded by a strong password.

The malware collected information about devices inside the company, while also still performing its video functions, periodically sending that data to an external website.

ultimate attack on corporate data privacy and security. A successful ransomware attack can paralyse a system—and, potentially, a company. The most common way for these attacks to occur is by getting someone to run infected software on the company's computers. The best way to eliminate that chance is to use a security strategy that relies on a cohesive—and up-to-date—set of endpoint, firewall and IDS/IPS tools.

Low-and-slow Attacks

In contrast to attacks that try to barge in via a firewall or email, a whole new breed of attacks can be described as low-and-slow intrusions. Instead of malware running on a computer, these attacks are funnelled through low-level applications or devices, like surveillance cameras, and are deliberately programmed to avoid detection by exfiltrating data slowly over time.

These attacks use a variety of ways to harvest data. A Tolly Group evaluation of low-and-slow attacks in 2019 found that, in one case, malware had compromised the OS of a surveillance camera. The malware collected information about devices inside the company, while also still performing its video functions, periodically sending that data to an external website. Since many firewalls are configured to assume outgoing traffic is legitimate, the information was exfiltrated successfully.

In another example, exfiltration software was contained in an unregistered Google Chrome browser extension.

Residing as part of the browser, it was able to gather data, which it then exfiltrated to an external website. Another incursion involved code that used the DNScat tunneling tool to take data files from the PC and send them to the attacker's website, which evades perimeter security in the process.

To deal with these kinds of threats when protecting your data, consider adding a new type of security system: a network detection and response (NDR) system. Unlike IDSes/IPSes that look for signatures, NDR systems use AI and machine learning to monitor network as they learn to understand normal traffic. An NDR system will detect anomalous traffic and alert corporate security teams to stop a low-and-slow exfiltration if it attempts to contact an external website to deliver stolen data.

Consider DLP Tools

Consider ways to keep tabs on data. One way to do that is to use data loss protection (DLP) software. DLP generally relies on an agent that runs on every client device. The software runs in conjunction with a management server and uses templates that identify data that needs to be protected from removal. Typical examples include data strings, like Social Security or credit card numbers.

Templates can also be created to flag certain keywords, such as trade secret or proprietary, to ensure documents containing these terms are protected. Generally, template-based DLP tools work best on structured data or files containing evident examples of confidential text.

Newer DLP products use features that examine the movement of all data rather than examining specific data patterns. These tools don't intercept data; rather, they create a trail of evidence to enable security teams to remedy leaks by pinpointing who may have exposed the data and the type of information revealed.

The Partnership Data-security Conundrum

When data gets compromised, there is little solace in saying, "It wasn't us. It was our partner." Keeping systems and data secured can be difficult when they are controlled by a partner. Indeed, the most serious problems organisations face may stem from lax security on the part of partners—businesses or cloud storage providers—with whom they share or deposit data.

Today's commerce almost requires companies share important data files with their business partners. But those partnerships also include risks in terms of data security threats. More than 12 million patients who used Quest Diagnostics had some of their medical records stolen when hackers accessed a contractor's IT system between 2018 and 2019.

The contractor, American Medical Collection Agency, was used by both Quest and LabCorp to handle billing collections. More recently, Amazon subsidiary Ring said some customer accounts were stolen by hackers who accessed an unidentified third-party service.

Equally worrisome, cloud providers aren't immune from problems. The so-called Cloud Hopper hack, revealed at the end of 2019, gave hackers unfettered access to data from a myriad of clients. Security analysts have confirmed trade secrets and other intellectual property were contained in stolen files. The victim companies had assumed their cloud storage vendors had adequate security. Bottom line: Don't assume files handed over to SaaS vendors are safe. They may not be.

Profitable data—be it credit card records, Social Security numbers or any other transactional information—will always be the target of motivated hackers. All they need is one way in. Keeping up with new hacking techniques and new safeguards, as well as constructing a strong security foundation, is the best way of protecting against data security threats. ■

Security And Privacy By Design: A Matter Of Corporate Social Responsibility For Tech Firms

IoT (and the data revolution more generally) exposes a plethora of potential new attack surfaces. Ultimately, the corporations implementing these new technologies bear the responsibility. Security and privacy must be baked into the core of all connected and data-generating / utilising products and services.

By JC Gaillard, Founder and Managing Director of Corix Partners

For years, many technology firms have treated security and privacy matters as an afterthought. It was at best a necessary evil related to regulations and compliance; at worst, something companies would window-dress in front of the few clients who would ask the question. It was seen as something boring and expensive, preventing innovation and at odds with functionality.

Of course, with the convergence of the Internet of Things (IoT), big data and cloud computing, the cards are now dealt quite differently. Many tech companies—large and small—are starting to realise that they are going to have to adjust their mindset to survive and to make the most of the times ahead.

IoT Data Invokes The Need For More Corporate Accountability

The convergence of these technology streams generates countless use cases in all industry sectors and has the genuine potential to transform our lives and create trillions of dollars of economic value. But, it also requires a type of hyperconnectivity that exponentially multiplies attack surfaces and is highly vulnerable to cyber threats.
"Data" is currently treated by many tech firms as a free limitless commodity. Many of those firms talk about it as if it belongs to them. But in practice, many firms acquire data through one-sided business deals and from consumers and citizens who have rights and the expectation of privacy. It's only a matter of time until such practices start to be challenged.

Security features have to be treated, designed and tested as proper product functionalities embedded as early as possible in product development. The respect of customers right to privacy has to be treated as a key business model parameter, not as something firms will compromise to make the numbers add up.

The digital transformation of society will never realise its full potential as long as the trust of consumers and citizens is constantly being weakened by data breaches, cybersecurity incidents and ruthless data monetisation by shameless vendors.

Technology vendors who want to stay in the game in the long term must take security and privacy seriously, and turn that into a competitive advantage for the generations of customers who share those values.

But it will be a massive cultural shift for many tech firms.

Responsible IoT Through Security And Privacy By Design

"Security by Design" and "Privacy by Design" principles have been established for some time. These principles are at the heart of what needs to be done to move forward.

Security features have to be treated, designed and tested as proper product functionalities embedded as early as possible in product development. The respect of customers right to privacy has to be treated as a key business model parameter, not as something firms will compromise to make the numbers add up.

The fundamental need for controls and the ethical treatment of customers at the heart of these principles may not be something tech executives were taught in business school. It's unknown if the current generation of executives, investors, marketers, and technologists running these firms are capable of understanding and delivering such a shift in values is a key factor.

Nevertheless, it is the ability of these firms to embrace these "Security by Design" and "Privacy by Design" concepts that will become the cornerstone of the digital transformation.

Fail to make the move and, at best, value creation will be reduced by several trillion (between one and three trillion by 2020 according to McKinsey & Co). In practice, if the trust of the people is irreparably damaged, the dynamics of the digital transformation may need to be reconsidered.

With so much at stake, it's becoming a fundamental matter of corporate social responsibility for tech firms to take security and privacy values to heart. ■

Smart Technology And The Threat To Privacy

Many governing bodies within cities are effectively implementing smart tech. Smart city solutions help to improve our human environment needs, making life more comfortable for all.

By Susan Morrow, IoT For All

I remember once taking my young daughter to the cinema to see a modern version of The Jetsons movie back in the 1990s. The Jetsons had originally aired in the 60s; this was a modern take on the film. Even in the 90s, the Jetsons' life of flying cars in a "smart city" seemed futuristic. Now, 30 years later, life depicted in The Jetsons doesn't seem so sci-fi, anymore.

Data within the smart city is analogous to blood that courses through the veins of the city, giving life to the structures within. A smart city is smart because it works to better our human environment needs, such as more efficient energy systems and building, and transport. Our data feeds the analytics that drive the mechanisms behind the sustainable and efficient operations of the smart pieces of the city. To best see how, where, and why our data is being harvested and used, we can look to some current examples of how governing bodies within cities are implementing smart tech.

There are a number of very interesting smart city projects going on across the globe. They're not entire smart cities like the Jetsons lived in, but instead, they're uplifting or replacing existing facilities to use smart tech where it fits. The examples here are but a taster of things to come to a city near you.

Toronto City, Canada

Toronto, which has been voted one of the worst cities for commuters, has partnered with Sidewalk Labs, which is owned by Alphabet Inc. (of Google fame) to build Quayside in Toronto which is promising to combine forward-thinking urban design and new digital technology to create people-centered neighbourhoods that achieve precedent-setting levels of sustainability, affordability, mobility, and economic opportunity.

The project hopes to have its first human residents by 2022. A press conference on the project presented the initiative as being community-driven. That is, the focus of the design of Quayside is to be beneficial at the community and citizen level.

Notably, ex-privacy commissioner, Ann Cavoukian, who is the person who created the foundational principles of Privacy by Design, resigned as advisor to Sidewalk Labs when they announced that they could not guarantee that the data collected would be de-identified at the source.

Deidentification of data is a crucial part of a privacy-enhanced smart city. Data should always be minimally collected where possible. However, where this is not

applicable, de-identification of data should be a fundamental design remit. On a related note, Canada is one of a number of countries that have smart initiatives. The pan-Canadian "Smart Cities Challenge" offers financial packages of up to CAD 50 million to companies that can help to improve lives through smart technologies. Competition One has already chosen winners with the Montréal, Quebec, winning in the CAD 50 million category. The city is focusing on sustainable transportation alternatives, in particular to improve access to local food supplies.

Barcelona, Spain

Barcelona is at the forefront of smart city living. The smart initiative in Barcelona has outlined a data directive that places emphasis on data sovereignty, privacy, and security when designing smart city infrastructures. Barcelona is working in several

Data within the smart city is analogous to blood that courses through the veins of the city, giving life to the structures within. A smart city is smart because it works to better our human environment needs, such as more efficient energy systems and building, and transport.

areas to transform city services, including smart parking. The city initially embedded Fastprk, an intelligent parking management system. The Fastprk sensors alert drivers of available parking spots, which helps drivers to locate spaces quickly, reducing emissions. The Fastprk system is based on the Sentilo open source sensor and actuator platform. More recently, Barcelona has implemented the AppParkb system.

The city is also making use of DECODE, which stands for DEcentralised Citizens Owned Data Ecosystem. This looks at using citizen data for the wider benefits of the city populace but with privacy as a design remit. DECODE is an EU-funded consortium that is exploring ways that open data can be used in smart cities, like Barcelona. The remit for their connected service in Barcelona is to offer control to the owners of data.

Barcelona is partnering with an organisation called City Protocol, which describes itself as a "collaborative innovation framework." City Protocol is working in collaboration with cities across the world to ensure that citizen data is used in a beneficial way for all. The collaboration aims to create a consensus around protocols and to deliver advisories on the use of citizen data in smart initiatives.

Smart Nation, Singapore

Asia is an innovator in technology, and it is applying this innovation to many cities in the Asia-Pac region. One of the poster children for the smart city movement in Asia is Singapore. The initiative driving the Singapore smart city is called Smart Nation. The project covers many areas of city living, from health to eGovernment to transport. The Health Hub positions itself as a "one-stop online health information and services portal." A number of countries, including the UK, are attempting to create national health portals. The Singapore Smart Nation Health Hub is well on its way to establishing a central place for citizens to access health records and other health information. One of the key features of the hub is that it uses the Singapore citizen identity, SingPass, for access to the Health Hub. It also states that the system has a delegated access facility for patient carers.

Asia is an innovator in technology, and it is applying this innovation to many cities in the Asia-Pac region. One of the poster children for the smart city movement in Asia is Singapore.

Identity and smart cities is something that I have explored in an earlier post; it's a crucial backbone of a smart city. Digital identity in the smart city is a key that will open the doors (sometimes literally) of many smart systems. However, unless properly designed to work as part of a critical infrastructure, it could also be a major area of privacy and security issues in the city. ■

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
IFSEC International 2020	8 - 10 Sep 2020	London	United Kingdom	www.ifsec.events/international/	IBC
GSX 2020	21 - 23 Sep 2020	Atlanta	U.S.A.	www.gsx.org	IFC
ISC West 2020	5 - 8 Oct 2020	Las Vegas	U.S.A.	www.iscwest.com	OBC
IFSEC SEA 2020	20 - 22 Oct 2020	Kuala Lumpur	Malaysia	www.ifsec.events/kl/	1
IFSEC Philippines 2021	21 - 23 Jul 2021	Manila	Philippines	www.ifsec.events/philippines/	3

issuu.com/securitysolutionstoday

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

IFSEC INTERNATIONAL

8-10 SEPTEMBER 2020
EXCEL LONDON UK

SECURITY IS CRITICAL
IFSEC IS ESSENTIAL

Security threats are always evolving.
Today there are more challenges than ever before.

IFSEC International brings together security products and expertise to suit every business. Through a series of complementary physical events and digital content, we'll find you a comprehensive solution to fit your needs, while maintaining maximum cost effectiveness.

Find out more at **www.ifsec.events/international**

Co-located with

FIREX INTERNATIONAL | INTELLIGENT BUILDING EUROPE | FACILITIES SHOW | SAFETY & HEALTH EXPO | WORKPLACE WELLBEING SHOW

CTX COUNTER TERROR EXPO | WORLD COUNTER TERROR CONGRESS | AMBITION EPRR CONFERENCE & ZONE | FORENSICS EUROPE EXPO

By Informa Markets