JUL - SEP 2021

SECURITY SOLUTIONS TODAY

SECURING INFRASTRUCTURE FROM RANSOMWARE

How do we defend important infrastructure against dangerous cyber threats?

IN THIS ISSUE

3 **In The News**
Updates From Asia And Beyond

10 **Security Feature**
+ Managing Onsite Security with Advanced Access Control

+ Ransomware Prevention Begins with Securing Your Applications

18 **Calendar Of Events**

In The News

04 | Hanwha Techwin Launches five P series AI cameras in 2MP

CONTACT

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

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

EDITOR Muneerah Bee (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)

Vectors Credit: Freepik.com
Designed by Fawzeeah Yamin

SECURITY SOLUTIONS TODAY
is published quarterly by Trade Link Media Pte Ltd (Co. Reg. No.: 199204277K)
101 Lorong 23, Geylang, #06-04, Prosper House, Singapore 388399
Tel: +65 6842 2580 Fax: +65 6842 2581
ISSN 2345-7112 (E-periodical)

Exclusive Media Representative for China and Hong Kong S.A.R.

Judy Wang
Worldwide Focus Media Co., Ltd
Flat / Room 02, 7th Floor, SPA Centre
No. 53 – 55 Lockhart Road, Wanchai
Hong Kong S.A.R. China
E-mail: judy@worldwidefocus.hk

CONTACTLESS RFID READER LAUNCHED TO SUPPORT AXIS ACCESS CONTROL SYSTEMS

Axis Communications announces the global release (except in the Americas) of AXIS A4020-E Reader for secure and seamless touch-free entry, and designed to match Axis network door controllers and Axis credentials

Featuring a mullion-mount design, the flexible reader is able to fit in narrow spaces and door frame installations. It is ideal for use in harsh environments both indoors and outdoors as it is IP65, NEMA 4X, and IK07 rated. Additionally, it offers tamper detection, and built-in cybersecurity features to help prevent unauthorised access and safeguard the system.

Designed to meet specific system requirements, this smart reader supports most types of smart RFID card standards with 13.56MHz credential technologies. Furthermore, it supports Open Supervised Device Protocol (OSDP) and Secure Channel Protocol (SCP) enabling secure communications and connections. ■

GLOBAL SECURITY EXCHANGE (GSX) TO TAKE PLACE AS A HYBRID OF DIGITAL AND IN-PERSON EVENT

ASIS International, the world's largest association for security management professionals, will move its Global Security Exchange (GSX) 2021 to a hybrid experience with in-person and digital features that will happen from 27 to 29 September 2021.

The three-day event features daily global keynote and game-changer presenters as well as concurrent education sessions focusing on the most pressing issues faced by the security profession. This integrated event will be hosted in-person at the Orange County Convention Center located in Orlando, Florida as well as online via the GSX event portal.

"This past year left an indelible mark on how we gather, learn and network. We took these key learnings into consideration along with our new reality in re-designing the GSX experience," stated John A. Petruzzi, Jr., CPP, 2021 President, ASIS International. "The event will showcase content related to how the world has changed and how we need to evolve our thinking around global security and safety in protecting people, property and intellectual assets. Another priority for us was to expand GSX offerings on a global scale so that security professionals anywhere in the world would have access to our best-in-class digital and in-person content and experience."

The GSX educational lineup addresses the most pressing topics and challenges to today's security professionals.

Attendees will be able to curate their experience, whether attending in-person or digitally, to advance their knowledge and understanding around these subject areas.

GSX 2021 will include more than 80 education sessions covering a range of topics from national security to community safety. Registrants will be able to choose how to connect to the GSX experience. All-Access in-person registrants will have access to pre- and post-show exclusive content. The digital audience will enjoy access to a broadcast studio format, watching some sessions live with the in-person audience, exclusive live interviews, and on-demand sessions.

"In developing GSX 2021, we recognise that security professionals are straddling two worlds simultaneously — physical and virtual," stated Peter O'Neil, FASAE, CAE, CEO, ASIS International. "While many professionals are focused on the health and safety of global citizens, security professionals are an essential element of that and more. By offering a truly integrated approach, GSX 2021 promises to be an event of the highest quality for the security profession."

For more information about GSX 2021, visit www.GSX.org ■

HANWHA TECHWIN LAUNCHES FIVE P SERIES AI CAMERAS IN 2MP

Global security company Hanwha Techwin recently launched a premium lineup of Wisenet P series artificial intelligence (AI) 2MP cameras with AI-enabled features.

The latest lineup of five cameras (PNB-A6001/PNO-A6081R/PND-A6081RV/PND-A6081RF/PNV-A6081R) captures quality images at up to 2MP resolution while including powerful, in-camera deep learning algorithms for advanced object detection, classification and error-free analytics. Utilising object recognition versus motion detection eliminates false alarms while also providing valuable business and operations insight.

The new cameras detect and classify objects including people, vehicles, license plates, and faces. It is equipped with a 'BestShot' feature which selects the most suitable image of classified objects to be sent to a backend server. Unique attributes of the objects are also stored as metadata alongside the video information including: colors of clothes, age groups, vehicle types, and colours. This prevents server overload and allows prompt AI-driven search for extracting information on specific objects, improving the overall search efficiency.

They also support the latest noise reduction technology, WiseNRII (Wise Noise Reduction II), which utilises AI object detection technology to identify object appearance or movements and

POWERFUL WAYS TO OPEN NEW DOORS

Altronix®

Designing and deploying access control has never been easier with Altronix power integration solutions. Create more ROI and leave the heavy lifting to us.

YOUR AMERICAN BRAND FOR **ACCESS POWER & CONTROL**

remove motion blur adaptively in low light environments with large amounts of noise. It effectively resolves the issue of blurry images and other effects caused by excessive noise reduction.

Wisenet P series AI 2MP cameras also support the company's proprietary WiseStreamIII technology. It identifies key objects such as people and/or vehicles based on the edge-based AI and compresses background data drastically.

This curtails data size and minimizes bandwidth for better operational efficiency in managing data storage. "The new lineup of 2MP AI cameras will offer greater access to diverse environments and applications," said

an official from Hanwha Techwin. "Our company will leverage its technical prowess to advance AI-powered solutions and diversify the product line, spearheading the rapidly growing AI market." ■

HID GLOBAL ADDS CLOUD-BASED MULTI-FACTOR AUTHENTICATION TO ITS WORKFORCEID UNIFIED IDENTITY AND ACCESS MANAGEMENT PLATFORM

Security company HID Global recently announced the latest addition to its cloud platform for creating a seamless, effortless experience for issuing, managing and using identity credentials in physical and digital workplaces, the Workforce ID Authentication.

It builds upon HID's multi-factor authentication platform for consumer applications, as part of a suite of employee ID badging, visitor management and workforce identity solutions.

"A person's identity has become the new security perimeter in a hybrid workplace that now extends from home to the office and everywhere in between," said Julian Lovelock, VP Global Business Segment, IAM, with HID Global. "The addition of multi-factor authentication to the HID WorkforceID platform advances our vision of a unified and flexible approach to identity and access management for an organisation's employees, partners and contractors. This is the next step in providing a suite of applications that manage digital and physical identity credentials through one convenient cloud platform."

The HID WorkforceID Authentication solution enables organisations to extend a streamlined, simple and secure

Image: www.freepik.com

login experience to every user and application throughout today's diverse and dynamic enterprise environment. It easily integrates with Microsoft's on-premise Active Directory (AD) or cloud-based Azure AD.

This standards-based security platform is positioned within the environment to enable simplified deployment and administration, multiple authentication factors, with an intuitive user experience. ■


GSX
GLOBAL SECURITY EXCHANGE
27-29 SEPTEMBER 2021
ORLANDO, FL, USA | ONLINE
GSX IS YOUR
BEST PLAY
If security is an endless game of offense and defense, the stakes have never been higher. New risks require new rules of engagement. Your next move? Registering for GSX—where security management professionals from every industry and sector discover winning strategies for return-to-work, asset protection, crisis management, and more.
REGISTER NOW AT GSX.ORG/SST1

PANASONIC LAUNCHES I-PRO S-SERIES FEATURING AI CAPABILITIES AT THE EDGE

Panasonic recently unveiled its enhanced i-PRO S-Series range of security cameras, featuring built-in artificial intelligence (AI) processors that enable the cameras to function as edge computing devices and deliver enhanced image quality in low-light conditions.

The series is the first mid-range line of security cameras by Panasonic to incorporate built-in AI capabilities, and it enables businesses to increase the speed and efficiency of their surveillance activities by reducing demand for bandwidth and infrastructure with data processing and real-time analytics taking place at the edge.

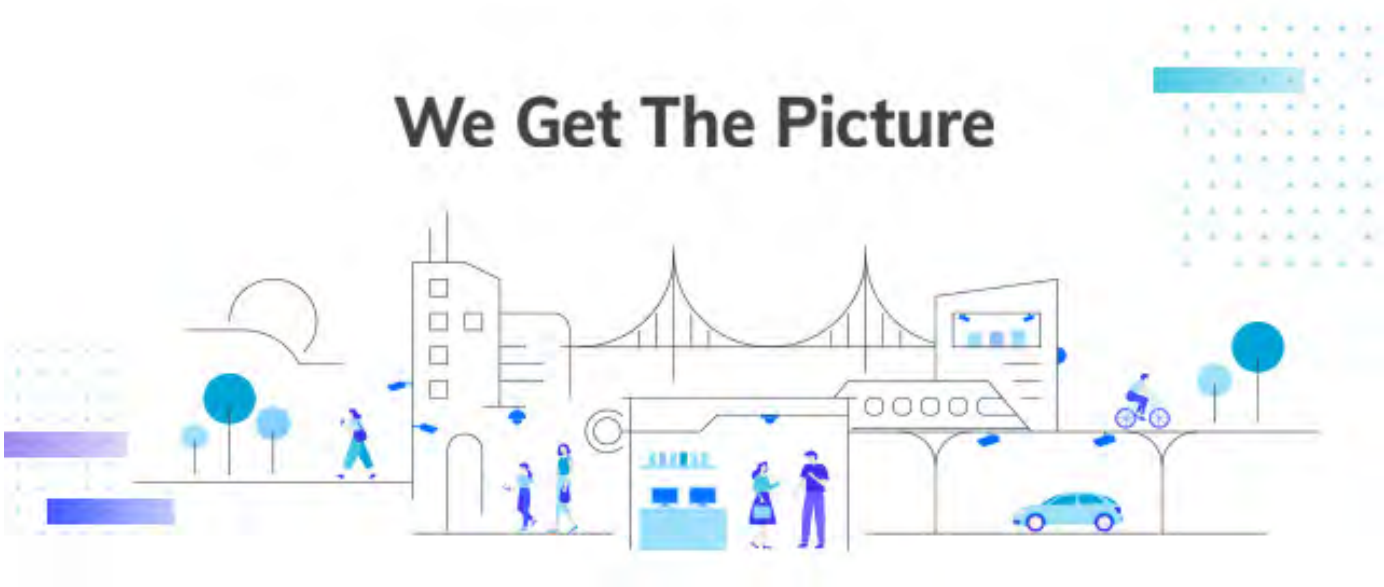
"As demand for edge computing and AI devices continues to grow, we see tremendous potential for Panasonic to set a new standard for security cameras with the launch of our i-PRO S-Series range. By pushing the limits of what traditional mid-range security cameras can do, the in-built AI capabilities of the i-PRO S-Series will allow more businesses to experience the power of edge computing, while enhancing the speed and efficiency of their surveillance activities to create a better and safer work environment for everyone," said Alvin Quek, Head of Security Solutions, Panasonic System Solutions Asia Pacific.

The i-PRO S-Series range of security cameras comes pre-bundled with in-house applications such as the AI-Video Motion Detection (AI-VMD) and AI Privacy Guard. These applications provide instant access to intelligent security functions such as intruder or loitering detection, while making sure that the personally identifiable information (PII) of individuals is protected through automatic pixellation of their figures and faces. This way, consumer privacy is prioritised, and the management of personal data is in compliance with geographies that have strict privacy laws, such as in Singapore with its Personal Data Protection Act (PDPA).

In addition, users of the i-PRO S-Series range of security cameras can leverage three other complimentary applications - AI Face, AI People and AI Vehicle Detection to enable quick searches of video footages based on pictures of faces (even with their masks on) or other pre-defined attributes of people and vehicles. These applications enable businesses to further harness AI, and go beyond the use of image recognition to leverage sound classifications picked up by external microphones, such as sounds of yelling, vehicle horns or glass breaking.

The Panasonic i-PRO S-Series range of security cameras will be available in Singapore from early July 2021 via authorised distributors. ■

VIVOTEK ANNOUNCES REBRAND, REVEALS COMMITMENT TO "GET THE PICTURE"



Global Internet Protocol (IP) surveillance solutions provider VIVOTEK recently unveiled its new branding in its transformation towards the Internet of things (IoT) age, including logo, brand identity, and a new brand ethos under the slogan "We Get The Picture."

The rebrand enables the company to take a more holistic approach and provide leading technology and intelligent insights. The new brand identity reveals its new style with a modern, user-centered, and digital friendly design.

Alex Liao, the president of VIVOTEK, stated: "When we say, 'We Get The Picture', it means to understand the whole situation in a prompt manner, and to always be a step ahead to deliver the solutions demanded by our end-users.

During the rebrand journey, we discovered that the way we did business for the last two decades, with outstanding service and business integrity, has profoundly shaped who we are today. Our new positioning and look redefine our role in the next era of IoT, but more importantly, deliver the clear message to our customers and partners that they can trust and stand side by side with VIVOTEK."

Founded in 2000, VIVOTEK established its headquarters in Taiwan and has concentrated on IP surveillance since inception. The company says it has been highly attuned to advancements in internet and surveillance in recent history. VIVOTEK will continue its tradition of research, development and user focus, and also move towards developments in the IoT. ■

Managing Onsite Security with Advanced Access Control

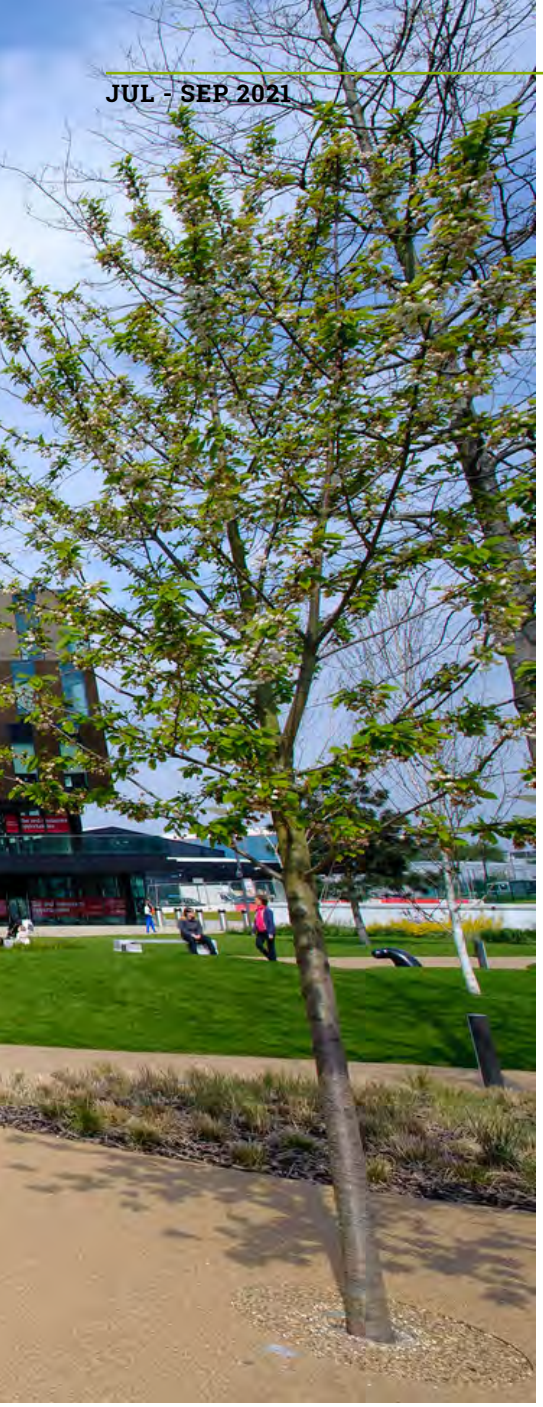
What does it take to secure a massive business park that is home to media giants such as the global broadcaster BBC? *We take a look at how MediaCityUK manages access control across the venue with upgraded systems in place.*

MediaCityUK, an international hub for technology, innovation and creativity located at Salford Quays in England is home to companies such as the BBC, ITV, Ericsson, dock10 and Kellogg's. These are complemented by more than 250 smaller media and digital businesses, all using advanced contactless access technology from security system supplier SALTO to provide site wide security.

Developed as a joint venture between Peel Land and Property Group (Peel L&P) and Legal and General Capital, MediaCityUK was designed around the specific needs of the media and creative industries, and the bespoke community features one of the biggest HD studio complexes in Europe; commercial offices; apartments; retail units, two hotels and a spectacular waterfront public piazza.

Peel Media Group's Head of Security Tony Chebrika and consultant Richard Sumner of RS Security Consultants (who has been working with Peel L&P since 2015) share how their access control solution is used to manage this diverse site.

What types of door are you controlling – internal or a mix of internal and external?



Tony: It's a mix of both types. We're using SALTO readers to control road blockers, gates and barriers, wall readers to control main entry doors and mostly XS4 handle sets to control internal doors.

Other onsite users such as SIS (Sports Information Services) have their own individual SALTO solution but also have access to MediaCityUK doors i.e. they carry access permissions on one card for two systems. This is the same for ITV who also run their own system.

All doors, whatever their location, are mainly accessed via contactless cards but we're also using SALTO's JustIN Mobile with Bluetooth Low Energy (BLE). This enables a smartphone to be used as the access credential for the electronic lock on the door. The mobile key is sent 'Over the Air' (OTA) to a JustIN Mobile app installed on a registered and verified smartphone. The user receives a message that they have a new key and for which doors they have access rights. They can then present their smartphone to the lock to gain access via the JustIN Mobile app.

All doors, whatever their location, are mainly accessed via contactless cards but we're also using SALTO's JustIN Mobile with Bluetooth Low Energy (BLE). This enables a smartphone to be used as the access credential for the electronic lock on the door.

You've recently designed a new security system – what did this involve?

Richard: Yes, the existing solution was all proprietary making it difficult

Based on an operational requirement and an evaluation of the product sets in the marketplace, Tony and I selected product sets that would not only meet our requirements today but considered a road map that would enable the systems to grow as developments came on board.

to operate, what it needed was a unified security system and a unified control room. So having tendered for the work I began working with Tony and his team. Based on an operational requirement and an evaluation of the product sets in the marketplace, Tony and I selected product sets that would not only meet our requirements today but considered a road map that would enable the systems to grow as developments came on board.

We selected SALTO as the access control solution plus IP Video Management Software firm Meyertech, Wavestore, AXIS cameras, 2n Intercoms and Siklu Wirelss links. It was my task to procure and manage the new security upgrade which would include new cabling, software and IP cameras site wide tied into a new state-of-the-art control room.

The goal of the upgrade was to implement event driven alarms and recordings. This would operate through a single user interface, which would enable control of all existing standalone systems across multiple sites so the new control room could see at a glance how and when people moved around all the different buildings.

SALTO was integrated with Meyertech and the wireless handle equipped doors - which operators can remotely lock and unlock - as part of the project as this was a first for both parties

and the end results are fantastic with a solution that meets the end users requirements on driving alarms and isolation of doors through a single front end GUI.

This means when a door is accessed, the camera is activated to provide a visual recording which can be used alongside audit trail data from the door itself. Another useful feature is that when a door alarm goes off, for instance in the case of a door being left open or forced, the camera system can display footage from five seconds before and five seconds after the event – making it possible to identify the culprit and then begin tracking them through the rest of the system.

Did sustainability and environmental considerations play a part in the decision making?

Tony: Yes our legacy matters so we take great pride in the way we go about our business and look to develop a long-term, sustainable future. In fact Peel L&P has recently been awarded a silver medal for its sustainability achievements placing it in the top 10% of participating global companies specifically for its environmental performance.

This cuts across to our suppliers too. It's important for us to ensure that the companies we work with share our values and SALTO, like us, takes its environmental responsibilities seriously. Their factory headquarters has achieved the feat of going entirely carbon neutral, the electricity used in manufacturing their products is generated by on-site solar panels or purchased as certified green electricity and they lead the way in the delivery of sustainable access control solutions by providing customers such as ourselves with smart lock products that reflect our own environmental values.

Is support for your access system provided by the company, by an approved partner or do you self support with your own trained staff?

Tony: We took a great deal of care when evaluating and selecting our access control system so what we have is reliable and any issues are minor and few and far between. When it comes to technical support, routine maintenance, troubleshooting and so on, we self support with trained MediaCityUK staff but can call on additional support from SALTO as the manufacturers as and when we need to do so.

MediaCityUK is a continually developing site and as new buildings and facilities are added further electronic locks and other security measures will be installed to control access to them.

Is there more development still to come at MediaCityUK?

Tony: Yes, MediaCityUK is one of the fastest growing communities in the UK, and we are committed to ensuring it remains a safe and secure destination where everyone is welcome. MediaCityUK is a continually developing site and as new buildings and facilities are added further electronic locks and other security measures will be installed to control access to them. Our community of workers and residents have been made aware of the new security improvements outlined above and they have been suitably impressed by the upgraded systems now in place.

Tell us about the awards that have been won for work on this project?

Tony: Richard's long-term work with me as Head of Security Peel Land & Property, Peel Retail Parks and MediaCityUK has been recognised on a couple of occasions. At the Association of Security Consultants 2020 awards he was presented with the Mike Cahalane Award which is presented annually to an independent security consultant for consultancy work and to highlight and recognise the positive difference independent security consultants can make in the public and private sector. And this year, at the first-ever virtual UK Outstanding Security Performance Awards (OSPAs) he won the Outstanding Security Consultant award.

Finally, can you summarise what access control provides for MediaCityUK?

Richard: Access control has been a major consideration from the very first brief on this project due to the size of the development and its future expansion potential. A smart 'keyless' environment was always a prerequisite to control access and it gives Tony full control over his security requirements. To date the SALTO solution has worked well and provides effective, secure, simple to manage access control in multiple buildings across the site. ■

Ransomware Prevention Begins with Securing Your Applications

By Taylor Armerding, Security Advocate, Synopsys Software Integrity Group

Ransomware isn't a new problem — not even close. It's been around for more than 30 years. But like every element of technology, it has evolved. Instead of being an occasional expensive nuisance, it's now a plague with existential implications for critical infrastructure — energy, transportation, food supply, water and sewer services, healthcare, and more.

The recent headlines have been a constant reminder of how vulnerable the owners and operators of that infrastructure — most of them private companies — are to ransomware attacks.

The state of ransomware attacks

The May 2021 attack that prompted Colonial Pipeline in the US to shut down its 5,500-mile pipeline, cutting off nearly half the fuel supply to the US east coast for the better part of a week, is just one ominous example. Because as modern ransomware attacks go, this one was fairly standard.

DarkSide, a ransomware-as-a-service group reportedly operating in Russia, didn't just encrypt data. They stole it as well, which puts more pressure on victims to pay since there's a threat of intellectual property and private customer information going public.

DarkSide, a ransomware-as-a-service group reportedly operating in Russia, didn't just encrypt data. They stole it as well, which puts more pressure on victims to pay since there's a threat of intellectual property and private customer information going public.

But the group attacked the company's IT network rather than the more sensitive operational technology (OT) networks that control the pipeline. That gave a measure of credibility to DarkSide's claim a few days later that, as Reuters put it, they were out for "cash, not chaos." In a statement posted on its website, the group said, "our goal is to make money, and not creating [sic] problems for society."

They added that the group is "apolitical" and should not be linked with any government.

Still, the attack created problems well beyond the ransom Colonial ended up paying — a reported US$4.4 million — although the Department of Justice announced June 7 that it had been able to recover about US$2.3 million of that by tracing and seizing the bitcoin wallet used by the hackers.
But at the time, the company shut down the pipeline "out of an abundance of caution" since it didn't know if the attackers had penetrated its OT systems.

Ransomware impact on critical infrastructures

The impact of the Colonial attack was anything but standard. It cut off multiple fuel supplies — gasoline, diesel, jet fuel, and heating oil — which led to panic buying and major price spikes. And it demonstrated yet again what multiple experts have warned for decades: Criminals or hostile nation states don't need bombs, missiles, or bullets to damage an adversary. They can do it with keystrokes on a computer.

Past illustrations of that reality include the Aurora demonstration in 2007 at Idaho National Laboratories, which destroyed a large diesel generator; Stuxnet, which destroyed a significant portion of Iran's nuclear facilities in 2010; and Industroyer, which brought down a portion of the energy grid in Ukraine in 2016.

But the Colonial attack was at an entirely new level, at least in the US Robert Lee, CEO of the cyber security firm Dragos, told Wired magazine that "this is the largest impact on the energy system in the United States we've seen from a cyber attack, full stop."

Government response to ransomware

So why aren't governments and the private sector organisations that are the targets of these attacks going on what would amount to a wartime footing to fight back?

Well, they are — sort of. The White House issued a memo this past week urging business leaders to act immediately to improve their resistance to ransomware attacks.

"The threats are serious and they are increasing," wrote Anne Neuberger, President Biden's deputy national security advisor for cyber and emerging technology.
Biden has also promised to confront

Russian President Vladimir Putin when they meet later this month about that country being a safe haven for ransomware criminals.

But if there's any good news, it's that the ways to resist ransomware attacks are well established. And while nothing will make an organisation entirely bulletproof from skilled, determined attackers, there are ways to make a successful attack much more difficult.

Ransomware security best practices

The following list includes the recommendations in the White House memo:

- **Build, maintain, and distribute secure software:** While the Colonial attack was enabled by the theft of a password, better software security is still the most effective defence against hackers. That means all the software — what an organisation builds itself and what it acquires from other vendors or from the open source community. Rehan Bashir, managing consultant with the Synopsys Software Integrity Group, said it takes "a holistic security approach — network, host, and application development. Organisations must adopt secure development processes that will produce secure software products and applications." That requires a secure software development life cycle (SDLC) where "security is an inline function of the development pipeline rather than an out-of-band activity," he said. An SDLC should start with architecture risk analysis to find and fix design flaws, and threat modeling to identify the ways malicious hackers might attack. Next, use application security and quality analysis tools. Throughout initial software development and updates, automated application security tools for static, dynamic, and interactive application security testing along with software composition analysis will help developers find and fix known vulnerabilities and potential licensing conflicts in open source software components. At the end of development, penetration testing can mimic hackers to find weaknesses that remain before software products are deployed. If an organisation needs more expertise or capacity, managed services providers can guide it through the process.

- **Back up data regularly:** Also, keep backups offline and not connected to the network. If backups are isolated and protected, an organisation can rebuild its system quickly at minimal expense. However, isolated backups won't protect an organisation from the modern ransomware attack that not only encrypts data but steals it as well, and then threatens to make it public if the ransom is not paid.

- **Build and maintain an inventory:** Identify all your assets. As the saying goes, you can't protect what you don't know you have.

- **Update and patch:** Failing to install an available patch for a known vulnerability is like leaving the door to a vault wide open.

- **Segment networks:** Ransomware attackers don't just steal and encrypt data. They also disrupt operations, which gives them more leverage with their targets. So organisations should separate their business functions from manufacturing/production operations, and limit internet access to operational networks. Especially with industrial control systems, it's crucial to isolate those networks so they can continue operating if the corporate network is compromised.

- **Train workers:** Most employees want to protect the organisation's assets. But if they fall for a phishing email, reuse passwords, or don't create complex ones, the best technology in the world can't protect against those failures.

- **Limit access:** While organisations should value all their employees, the reality is that the more people who have access to sensitive data, the greater the risk. Network segregation is the way to limit access to only what employees need to do their jobs.

Better security is an investment. It starts with a strong software foundation, continues with careful thought about firewalls and network design, and is maintained with constant vigilance, including monitors and secure software updates.

- **Limit plugins:** They can be an entry point. Either disable them or make sure they are updated regularly.
- **Verify, then trust:** All documents should have viewable file extensions from trusted sources. Don't let your system download irrelevant documents that may be coming from malicious sources.

Make application security a priority

For years, many organisations have complained that they have neither the time nor the money to implement those protections, and that hackers wouldn't be interested in them anyway.

That is, demonstrably, a very risky strategy. "Security by obscurity" doesn't work. And the cost of paying cyber criminals and recovering from a ransomware attack will be greater, by orders of magnitude, than any "savings" from failing to implement good security.

Better security is an investment. It starts with a strong software foundation, continues with careful thought about firewalls and network design, and is maintained with constant vigilance, including monitors and secure software updates.

You may never know the ROI from all this, but that's the point — you don't want to know. ■

COMING SOON

JUL 7 – 9 2021

Secutech 2021
Taipei, Taiwan
+886 2 8729 1099
https://secutech.tw.messefrankfurt.com
services@secutech.com

JUL 12 – 14 2021

IFSEC International
London, United Kingdom
+44 (0)20 7069 5000
www.excel.london/
info@excel.london

JUL 19 – 21 2021

ISC West 2021
Las Vegas, USA
+1 203 840 5602
www.iscwest.com
inquiry@isc.reedexpo.com

JUL 21 – 23 2021

IFSEC Philippines 2021
Manila, Philippines
+63 2 551 7718
www.ifsec.events/philippines
ifsecph@informa.com

AUG 25 – 28 2021

Secutech Vietnam 2021
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 27 – 29 2021

GSX 2021
Orlando, USA
+1 703-519-6200
www.gsx.org
asisfuture@asisonline.org

NOV 9 – 11 2021

IFSEC Southeast Asia 2021
Kuala Lumpur, Malaysia
+60 3-9771 2688
www.ifsec.events/kl
ifsecsea@ubm.com

NOV 24 – 26 2021

Secutech Thailand 2021
Bangkok, Thailand
+66 2 664 6488
www.secutechthailand.tw.messefrankfurt.com
stth@taiwan.messefrankfurt.com

JAN 16 – 18 2022

Intersec 2022
Dubai, UAE
+971 4 389 4500
www. intersec.ae.messefrankfurt.com
intersec@uae.messefrankfurt.com

SEP 20 – 23 2022

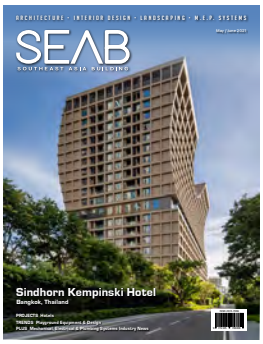
Security Essen 2022
Essen, Germany
+49 201 72440
www.security-essen.de
info@messe-essen.de

SUBSCRIPTION FORM

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

Please (√) tick in the boxes.

PRINT



☐ **Southeast Asia Building**
Since 1974

☐ **Southeast Asia Construction**
Since 1994

***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) per magazine*

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

DIGITAL

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

http://lt.tradelinkmedia.biz

☐ **Lighting Today**
Since 2002

Security Solutions Today
is available on digital platform.
To download free PDF copy,
please visit:

http://sst.tradelinkmedia.biz

☐ **Security Solutions Today**
Since 1992

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: _____

ADVERTISE WITH US TODAY!

Email us at info@tradelinkmedia.com.sg.

Scan to visit our website