Security Solutions Today

November / December 2018

WITH BAD NEWS PILING UP, SHOULD INDUSTRY RETHINK CYBER SECURITY?

Cover Focus

The Financial Sector Is Under Siege!

Cover Focus

The King Is In The House - And It's Called Malware

Inside Look

Test Drive Your Security Approach

Download our new Tradecards Global App on iOS and Android to read the latest issue!

Embrace Your Digital Transformation

Harness AI & BI to increase competitiveness with Dahua Smart Retail

< Facial Recognition >

< People Counting >

< Business Intelligence >

- Creates exclusive profiles based on face attributes, provides accurate customer segments for better targeted marketing strategy.
- Provides accurate statistics for people stay, conversion rate, customer flow analysis and traffic effected by weather, allowing retailers to optimize customer-to-staff ratio to reduce human resource cost.
- Structures all the data collected and generates daily/monthly/annual operation reports, easy for retailers to export or search.

CE FC ISO 9001:2000

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

SAVE THE DATE

ISC WEST
INTERNATIONAL SECURITY CONFERENCE & EXPOSITION

SPONSORED BY: SIA SECURITY INDUSTRY ASSOCIATION

APR 9-12 2019

SIA Education@ISC: April 9-11, 2019
Exhibit Hall: April 10-12, 2019
Sands Expo | Las Vegas
www.ISCWest.com

COMPREHENSIVE SECURITY FOR A SAFER, CONNECTED WORLD

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

CONNECTED SECURITY EXPO @ ISC WEST FEATURING:

&

UNMANNED SECURITY EXPO @ ISC WEST

www.ISCWest.com/Register

IN THIS ISSUE

CONTACT

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

EDITOR
Michelle Lee (sst@tradelinkmedia.com.sg)

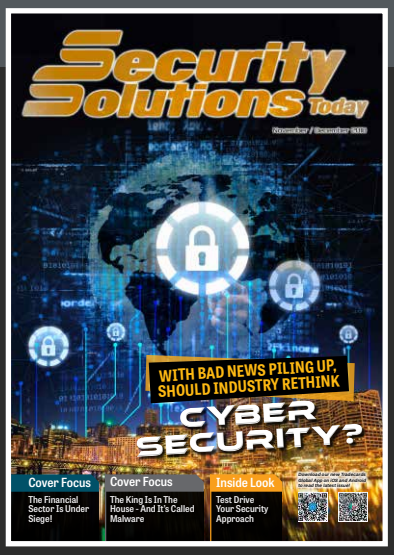
GROUP MARKETING MANAGER
Eric Ooi (eric.ooi@tradelinkmedia.com.sg)

MARKETING MANAGER
Felix Ooi (felix.ooi@tradelinkmedia.com.sg)

HEAD OF GRAPHIC DEPT/ ADVERTISEMENT CO-ORDINATOR
Fawzeeah Yamin (fawzeeah@tradelinkmedia.com.sg)

GRAPHIC DESIGNER
Siti Nur Aishah (siti@tradelinkmedia.com.sg)

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



Images/Vectors Credit: Pixabay.com / Freepik.com

Designed by Siti Nur Aishah

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

Printed in Singapore by KHL Printing Co Pte Ltd.

ANNUAL SUBSCRIPTION:

Surface Mail:

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

Airmail:

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

ADVERTISING SALES OFFICES

Head Office:
Trade Link Media Pte Ltd *(Co. Reg. No: 199204277K)*
101 Lorong 23, Geylang, #06-04, Prosper House,
Singapore 388399
Tel: +65 6842 2580 Fax: +65 6842 1523, 6846 8843, 6842 2581
Email (Mktg): info@tradelinkmedia.com.sg

China & Hong Kong
Iris Yuen
Room 1107G, Block A,
Galaxy Century Building
#3069 Cai Tian Road,
Futian District
Shenzhen
China
Tel : +86-138 0270 1367
sstchina86@gmail.com

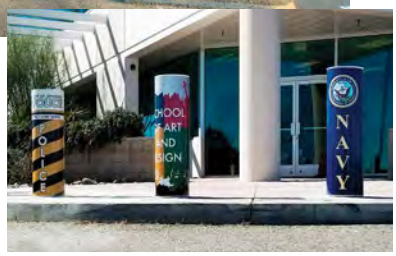
Japan:
T Asoshina/Shizuka Kondo
Echo Japan Corporation
Grande Maison, Rm 303,
2-2, Kudan-Kita,1-chome,
Chiyoda-ku, Tokyo 102,
Japan
Tel: +81-3-32635065
Fax: +81-3-32342064

THIS IS NO TIME TO GAMBLE!

Delta's Crash-Certified Vehicle Barriers— People's **Lives Depend** On Them Everyday!

It's a fact. Since 1974, Delta Scientific has established the safety standards for high security vehicle barricade systems—barricades, beam barricades, bollards, portable barriers, sliding gates, surface mounted barriers—parking control equipment and guard booths. Delta systems can stop a 16,500 lb truck going 50 mph (7500 kg @ 80 kph)...and keep protecting.

Delta is also the acclaimed industry leader for customer service and technical support...the foremost choice of militaries, embassies, capitols, colleges, law enforcement agencies, auto lots, parking structures, international borders, airports, municipalities, public infrastructures and courthouses from Riyadh to Washington, London, Singapore and Rio de Janeiro. From protecting Presidents to pedestrians, Delta systems stop terrorists dead.



Bet your life on Delta.

Ask about our NEW bollard covers!

DELTA

Visit **www.deltascientific.com** for details and specifications. ▲ **1-661-575-1100** ▲ **info@deltascientific.com**

COMING SOON...

DECEMBER

Counter Terror Asia 2018

Date: 4 - 5 December 2018
Venue: Marina Bay Sands, Singapore
Organiser: Fireworks Trade Media Pte Ltd
Telephone: +65-6100 9101
Website: www.counterterrorasia.com
Email: sg@fireworks.com

APRIL

ISC West 2019

Date: 9 - 12 April 2019
Venue: Sands Expo, Las Vegas, NV, USA
Organiser: Reed Exhibitions
Telephone: (800) 840-5602
Website: www.iscwest.com
Email: inquiry@isc.reedexpo.com

APRIL

Secutech India 2019

Date: 25 - 27 April 2019
Venue: Bombay Exhibition Centre, Goregaon (E) Mumbai, India
Organiser: Messe Frankfurt New Era Business Media Ltd
Telephone: +886 2 8729 1099
Website: www.secutechindia.co.in
Email: stid@newera.messefrankfurt.com

JUNE

IFSEC International 2019

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

JUNE

IFSEC Philippines 2019

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

OCTOBER

Secutech Thailand 2019

Date: October 2019
Venue: Bangkok International Trade and Exhibition Centre, Bangkok, Thailand
Organiser: Messe Frankfurt New Era Business Media Ltd
Telephone: +886 2 8729 1099
Website: www.secutechthailand.com
Email: stid@newera.messefrankfurt.com

MicroEngine®

Integrated Security Systems

The Trusted Brand in Security Solutions

xPortalNet HS

High Security System Software

- 20 Digits (Full DesFire 64-bit CSN and Card ID)
- DesFire Security Profile Configuration
- Alarm Monitoring & Lift Controller
- CCTV Integration
- Visitor Management System (VMS)
- Dynamic Floor Plan for Real-Time Monitoring
- Web Server Support

Projects


Commercial / Complex


Factory


Condominium

500+ doors access & security system on SQL Server for factory and many more...


Plato DesFire Reader

1300-88-3925 or enquiry@microengine.net

www.microengine.net

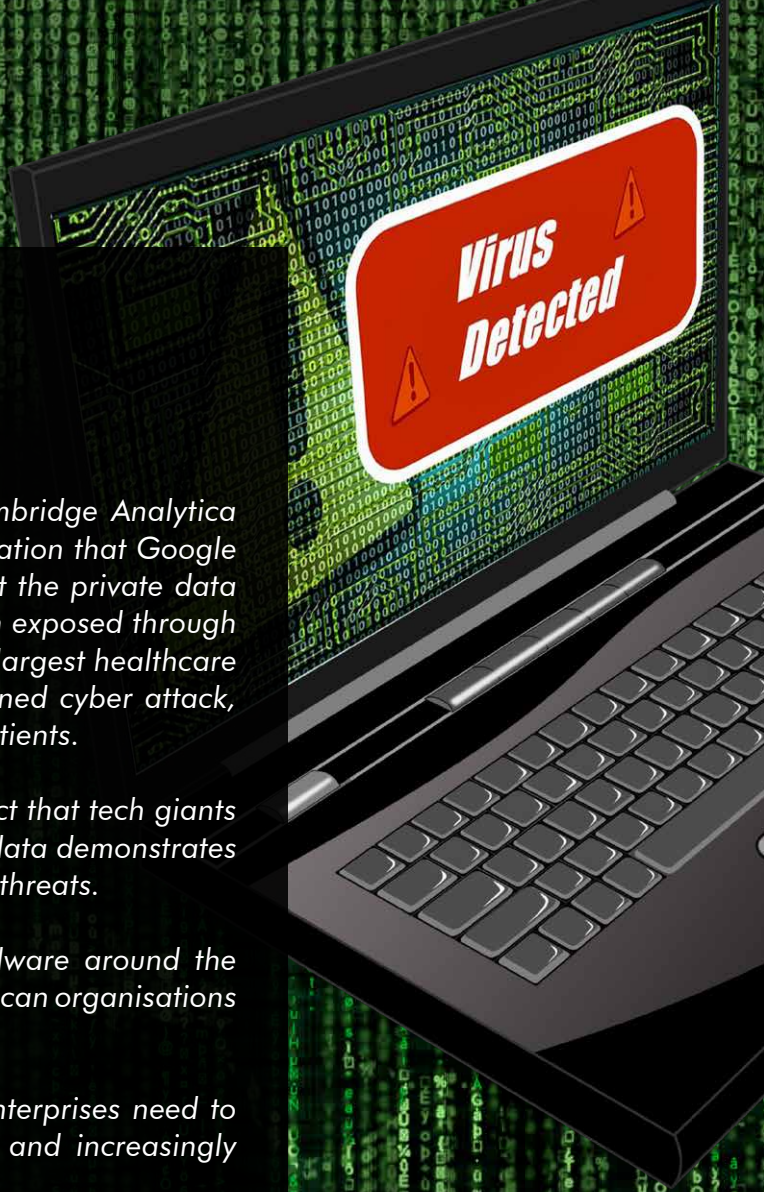

Our Office


Service Centre

GlobalGROUP ISO 9001 5965 UKAS MANAGEMENT SYSTEMS

REG No. 749921389

EDITOR'S NOTE



Dear esteemed reader,

The bad news just keeps coming.

The reports of Facebook's catastrophic Cambridge Analytica data breach were unsettling. Then came the revelation that Google quietly shut down Google+ after discovering that the private data of as many as 500,000 Google+ users have been exposed through a bug. In Singapore, the IT system of Singapore's largest healthcare group, SingHealth, was the target of a well-planned cyber attack, which led to the leak of the data of 1.5 million patients.

It all made one thing clear: no one is safe. The fact that tech giants like Facebook and Google could not secure their data demonstrates just how challenging it is to defend against cyber threats.

Today the explosive growth of hacking and malware around the world means that every enterprise is vulnerable. But can organisations reduce their vulnerability?

This issue focuses on the big question of what enterprises need to do to protect themselves against ever-changing and increasingly sophisticated cyber threats.

It's time to rethink cyber security, said several software and services companies. Prioritise cyber security actions, said The Center for Internet Security.

What is clear is that as data moves to more applications and devices than ever before, no organisation is safe from attacks. And with threats evolving at lightning speed, a proactive security posture is now more critical than ever.

Michelle Lee

Editor

ALTRONIX PACKS A 1-2 PUNCH!

TROVE STREAMLINES ACCESS CONTROL DESIGN AND DEPLOYMENT, INCREASING PROFITS AND ROI.

WINNING POWER COMBINATIONS – ENHANCING YOUR CUSTOMER'S SECURITY.

TROVE

Powered by Altronix

MADE IN THE U.S.A

CUSTOMIZE TROVE AT **ALTRONIX.COM**

ST Engineering, Cisco and IBM Team Up To Safeguard Cyber Landscapes

ST Engineering, Cisco Security and IBM have teamed up to develop integrated cyber security solutions that safeguard information technology (IT) and operational technology security (OT) networks in industrial control systems. The solutions will enhance the safe operations of critical infrastructures that deliver essential services including energy, aviation, maritime and land transport.

The three-party collaboration will combine the engineering capabilities, technical expertise in network security space and advanced analytics capabilities of the three technology powerhouses to develop an integrated and secure reference solution architecture. The architecture will guide companies in designing their cyber security infrastructure and help them counter cyber security challenges by integrating capabilities to secure both IT and OT networks. It will also provide a consolidated overview and analysis of cyber events to enable security teams to address cyber incidents more collaboratively.

The collaboration will see the integration of Cisco Security's solutions, IBM's QRadar platform as well as ST Engineering's technology and engineering expertise to deliver best-of-breed solutions. The three partners are also exploring building a Centre of Excellence to demonstrate and promote the offerings developed through the collaboration, including cyber security training and industry certification.

"In this fast-evolving threat landscape, cyber security needs to be an intricate part of any system or network design. We are confident that this unique and dynamic collaboration will develop robust solutions to help companies secure their networks," said Goh Eng Choon, General Manager of Info-Security, Electronics, ST Engineering.

According to the recent Cisco 2018 Asia Pacific Security Capabilities Benchmark Study, companies across Asia Pacific do not address half of the legitimate cyber threat alerts they receive. Among those surveyed, 53% of companies receive more than 10,000 alerts each day.

With the number of cyber threats increasing rapidly, the real challenge lies in the management of the process that takes place after the alert is received and the issue of how many are actually investigated. The study shows that on average only half of the alerts received are investigated.

Digital innovation and adoption is taking place at a rapid pace across Southeast Asia. However the success of digitisation hinges in a large part on the region's ability to tackle the cyber security challenge and develop local capability, especially talent pool, stressed Cisco.

"We need to remember that cyber criminals are constantly working together and are relentless in hacking networks and inflicting damage on their targets. Defenders need to take a similar approach by collaborating more, sharing intelligence and ensuring they stay a step ahead of the attackers," said Stephen Dane, Managing Director of Security for Asia Pacific, Japan and China at Cisco. SST

High Security Smartphone

In October, Bittium showcased its high security smartphone Bittium Tough Mobile at the Cyber Security Nordic event in Helsinki.

Designed and built for the demanding mobile security and public safety markets, the Android-based Bittium Tough Mobile is packed with innovative features that make it a perfect tool for users such as government agents, authorities, first responders and other professionals who need to communicate securely and reliably in critical communication situations. It's the first device to be certified to handle confidential information by the Finnish government.

Bittium Tough Mobile in tough in several ways. It has dust and shock protection. Its touchscreen works in wet conditions. And it incorporates a special hardware-based security platform with features like tamper detection, integrity check to ensure end-user security and privacy as well as deep integration of both customers' own and third party software security solutions.

By offering both a rugged digital setup and a physically rugged phone, Bittium hopes to conquer sectors where both the environment and the types of data being collected are challenging. SST

Bittium Tough Mobile™ - Secure and strong LTE smartphone https://www.bittium.com/BittiumToughMobile

"Asia's Premier Counter-Terrorism and Internal Security Exhibition and Conference!"

CTAX

COUNTER TERROR ASIA EXPO 2018

4 - 5 DECEMBER 2018

Marina Bay Sands, Singapore

Co-Located With:

www.counterterrorasia.com

An International Conference on Counter-Terrorism and Internal Security

For more info, contact us:
Phone: (+65) 6100 9101 | Email: sg@asiafireworks.com

Organized by:

FIREWORKS® TRADE MEDIA GROUP

Fireworks Trade Media Pte Ltd

Boon Edam Demonstrates Powerful Intrusion Prevention At GSX 2018

Boon Edam showcased several highest level security entrances at its booth at Global Security Exchange (GSX) 2018 in Las Vegas in September.

Among the access control systems on show were the Tourlock 180+90, Circlelock security portal and Circlelock Combi.

The Tourlock 180+90 integrates an AMAG Symmetry card reader into Boon Edam's best-selling security revolving door. This pairing of access control integration with high bi-directional throughput prevents tailgating and piggybacking without the need for manned supervision.

Meanwhile the Circlelock security portal offers the highest level of security available in an entrance for organisations looking to prevent intrusion into highly sensitive areas such as data centres. The Circlelock incorporates two-factor authentication with an AMAG Symmetry card reader on the outside of the portal plus an iris scanning technology from Iris ID to fully authenticate identity.

Also on show was Boon Edam's newest entry, the Circlelock Combi. This half-portal transforms an existing swinging door into a high security mantrap entrance that prevents piggybacking – saving both space and renovation costs. Visitors to the show were offered a demonstration of two-factor authentication for Circlelock Combi that involved an AMAG Symmetry card reader plus facial scanning technology from StoneLock Pro®.

This year, Boon Edam was again the official turnstile sponsor of GSX.

With the launch of its interactive troubleshooting guides for security entrances, a range of new partner technology integrations and bolstered by growing demand from the increasing adoption of anti-tailgating and anti-piggybacking entrances by Fortune 50 Global companies, the company is advancing its position as the market leader in the Americas in security entrance solutions.

"Boon Edam has held the top position for security entrances in the Americas since 2012 according to IHS Markit reports," said Greg Schreiber, Senior Vice President of Sales, Boon Edam, Inc. "Serving our customers and this industry with stronger, safer options for protecting entrances from tailgating and other unauthorised incursions will always be our first priority." SST

IFSEC
PHILIPPINES

SECURITY • FIRE • SAFETY

13 - 15 JUNE 2019

SMX CONVENTION CENTRE
PASAY CITY, METRO MANILA

Organised By

UBM

THE LEADING
SECURITY, FIRE & SAFETY
EVENT IN THE PHILIPPINES

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

WWW.IFSECPHILIPPINES.COM

@IFSECPHILIPPINES #IFSECPHILIPPINES IFSECPHILIPPINES

Breakthrough Low-light Cameras From Bosch

Bosch brings to the mid-range market a breakthrough product range in the AUTODOME IP starlight 5000i.

Built around starlight technology, this range of cameras is able to deliver colour images in conditions where other cameras are forced to switch to monochrome. This include extremely low-light settings as low as 0.018 lux. Combined with an excellent High Dynamic Range of 120dB, AUTODOME IP starlight 5000i cameras offer the highest image quality in the market today for mid-range moving cameras.

The cameras features Essential Video Analytics as a standard. This means the cameras understand what they see and immediately alert you to any potential threats. It also allows for instant retrieval of footage from hours of stored video. When idle, these cameras are able to analyse behaviour, assist in enforcing health and safety regulations (such as raising awareness of a blocked emergency exit) or churn out usable statistics such as the number of people going into a certain area.

In addition, the cameras boast Intelligent Dynamic Noise Reduction and intelligent streaming, combined with H.265 video compression. This reduces bitrate by up to 80%, keeping video data manageable while substantially reducing network strain and storage requirements. All without compromising video quality.

Like all Bosch network cameras, AUTODOME IP starlight 5000i cameras come with various software and hardware applications such as a built-in Trusted Platform Module, which keeps video data secure. IR and in-ceiling models are also available in the range. SST

OpenText Named Content Services Platforms Leader

OpenText, the global leader in Enterprise Information Management (EIM), was named a Leader for Content Services Platforms in Gartner's 2018 Magic Quadrant.

The company provides market-leading information management solutions on premises or in the cloud. Part of the OpenText EIM platform, OpenText Content Services help organisations readily access critical business content when, where and how it is needed.

This is the second consecutive year OpenText has been ranked a Leader for Content Services Platforms. The company has also been designated a Leader in the Gartner Magic Quadrant for Enterprise Content Management for 12 consecutive years.

"As companies embrace the power of AI, automation and IoT, the value and volume of data and content are rapidly increasing," said Mark J. Barrenechea, Vice Chair, CEO and CTO, OpenText. "OpenText has been investing heavily in this vision and our customers continue to benefit from our investment." SST

secutech
THAILAND

The premier security, fire safety and smart home & building trade fair for smart city developments in Thailand

October 2019
Bangkok, Thailand
www.secutechthailand.com

Global contact:
Messe Frankfurt New Era Business Media Ltd.
Jason Cheng
+886 2 8729 1099 ext. 215
stth@newera.messefrankfurt.com

Thailand contact:
Worldex G.E.C. Co., Ltd.
Sirapat Kettam (SK)
+66 2 664 6488 ext. 501
sirapatk@worldexgroup.com

WORLDEX
Group of Exhibition Companies

messe frankfurt

More Power Per Port From Altronix

NetWay8GP provides up to 60W per port and NetWay16G up to 30W per port

Altronix launched two high-powered additions to its industry-leading line of NetWay™ Midspans at Global Security Exchange 2018.

NetWay8GP 8-port Midspan provides up to 60W power per port to power PoE/PoE+/Hi-PoE devices (480W total). NetWay16G 16-port Midspan delivers up to 30W power per port for PoE/PoE+ devices (480W total).

"As IP devices continue to offer more features requiring higher power, our new NetWay Midspans provide the power and intelligence that today's networked systems demand," said JR Andrews, National Sales Executive of the leader in power and transmission solutions for the professional security industry.

The NetWay8G and NetWay16G both feature a 1U rack enclosure; 10/100/1000 Mbps data rates at distances of up to 100m; an integral battery charger for applications requiring backup; and embedded Altronix LINQ™ Technology to monitor, control and report power and diagnostics from anywhere. SST

secutech
INDIA

The road to India's security market

25 – 27 April 2019
Bombay Exhibition Center
Goregaon (E) Mumbai, India
www.secutechindia.co.in

Contact organizer
stid@newera.messefrankfurt.com

ABEC

messe frankfurt

Dahua Unveils Industrial Camera Range

The demand for industrial cameras is growing rapidly as a result of the increasing need for quality inspection and automation, growing demand for AI and IoT integrated machine vision system and the development of new connected technologies.

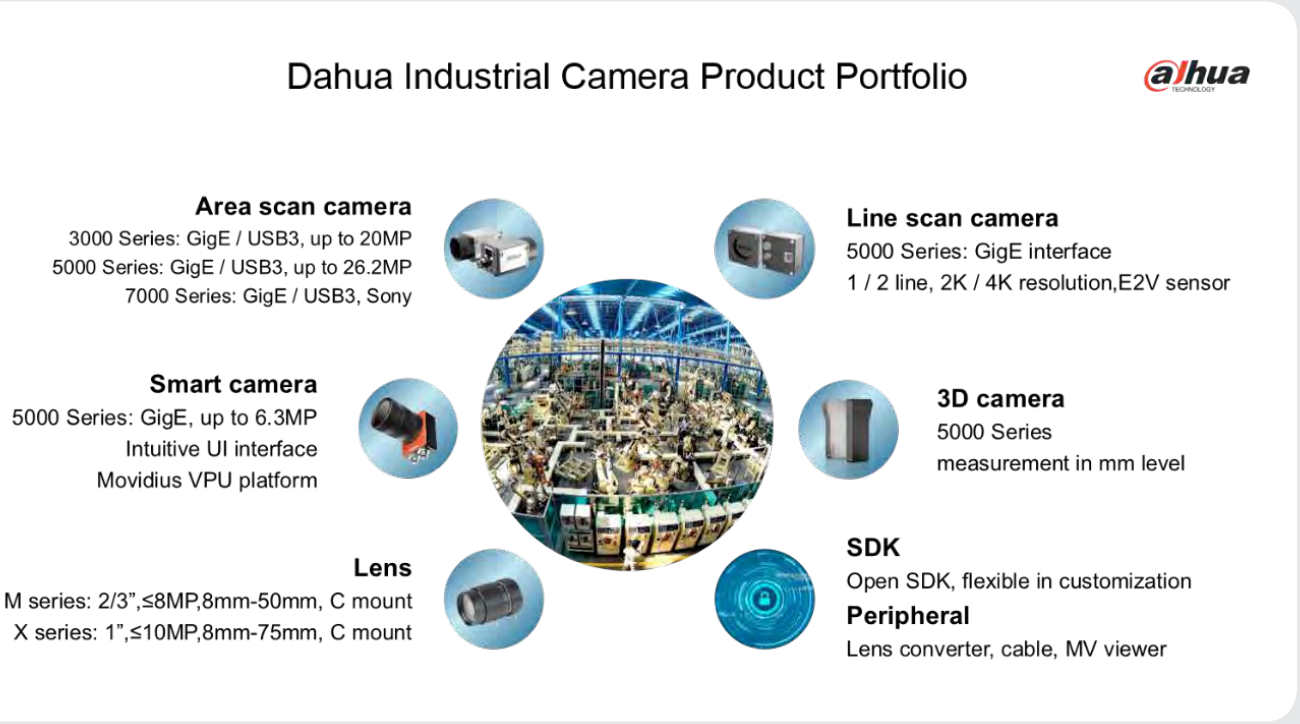
Industrial cameras are cameras designed to high standards with repeatable performance and robust enough to withstand the demands of harsh industrial environments. They are also known as machine vision cameras as they are used on manufacturing processes for inspection and quality control. They are used in many sectors from logistics and security systems to medical technology.

To meet this robust demand, Dahua Technology, a leading solution provider in the global video surveillance industry, has launched a series of new industrial cameras to enrich its product offerings for the logistics industry and general industry.

Dahua's new line-up of industrial cameras includes:

- Area scan cameras available in three product series: 7000, 5000 and 3000. The 7000 series is targeted at users who require the highest level of performance. The 5000 series strives for price-performance balance while the 3000 series is an entry level range for users looking for values. GigE and USB3 interface are available for the different applications.
- Line scan cameras: 1/2 line and 2K/4K line scan cameras are now available for different applications that require both high resolution and high scan rate with moving objects.
- Smart cameras: Dahua offers a Movidus-based smart camera with embedded sophisticated code-reading algorithm. This camera is intended for the logistic industry, particular in the field of logistic automation.
- 3D camera: Dahua recently added a 3D camera to its range that is able to measure objects at the millimetre level.
- Lens and peripherals: Dahua's range includes a wide array of lens and peripherals for complete industry solutions.

SST



Securing The World's First Underwater Quarry Hotel

ASSA ABLOY is providing total door opening solutions to the award-winning Shimao Wonderland Inter Continental Hotel in Shanghai, China.

While many hotels boast grand views from the world's tallest buildings, the pioneering five-star hotel is being built inside a quarry 100 meters below ground level with its bottom two floors under water. The impressive structure will be fitted with ASSA ABLOY-branded architectural hardware and Henderson's telescopic sliding doors. ASSA ABLOY Security Solutions customised high-end branded hardware, including concealed door closers, hinges and panic exit devices, in a dark bronze shade to suit the hotel's luxurious feel and colour scheme.

"The hotel's intricate design made the project challenging," said York Gong, sales manager of ASSA ABLOY Security Solutions. "The landmark building's hardware not only required a customised colour in line with the hotel's prestigious design, but also good visual appeal on top of functionality and security."

Designed by British firm Atkins under the leadership of renowned architect Martin Jochman, the groundbreaking project has already won a number of international awards, including the gold award for Chinese Future Architecture, the Best International Hotel Architecture and the Best Luxury Hotel Architecture, among others.

Work started in 2006 and is expected to exceed US$151 million by the time the interiors are fitted. The project's most impressive feature is a vertical glass atrium above the hotel disguised as an artificial waterfall. SST

Unassailable Browsing Solution Demonstrated at Cloud & Cyber Security Expo Singapore 2018

Few essential business activities are as risky as browsing the web. A whopping 80% of security breaches originates from browser and email threat vectors.

Following the recent hacking of Singapore's public healthcare system as well as increased awareness of the threat of ransomware, cryptojacking and other browser-borne attacks, it has become clear that current solutions just aren't enough, said Ericom Software.

Detection-based approaches can't reliably distinguish legitimate content from malware, said the leader in securely connecting the unified workspace. Site categorisation lets malicious code slip in on white listed sites. Both methods are reactive, deploying defensive measures only when a potential threat is detected. Plus they require frequent resource-intensive patches and updates.

Isolate Your Browser

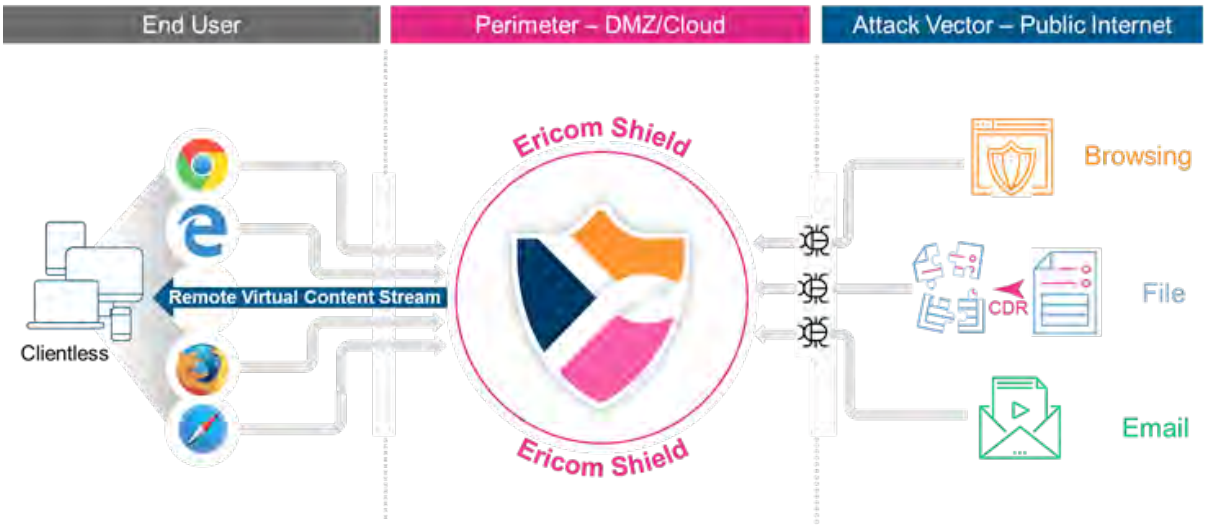
One solution proposed by Ericom Software is an Internet browsing experience that is completely isolated from the endpoint device. The company presented that solution in the form of Ericom Shield at Cloud & Cyber Security Expo 2018 in Singapore.

Ericom Shield executes websites and other web-based content in a remote isolated environment, inside a disposable Linux container. When the user closes a tab or stops browsing, the container is discarded along with all code picked up from the site – malicious and benign.

Ericom Shield adds a layer to defense-in-depth strategy by isolating malware, ransomware and other threats where they can't harm networks and user devices. Ericom Software promises that Ericom Shield will empower end users with full, transparent Internet use – including file downloads – while reducing risk, costs and operational burden. It ensures a smooth and seamless browsing experience from any standard browser and any device, using any OS, said Ericom Software.

Ericom Shield ensures the safety of all files downloaded from the web using factory-integrated Content Disarm and Reconstruction (CDR) technology to disarm downloaded content before releasing it to the user's device.

"Singapore is leading the region in adopting compulsory Internet separation. As security experts increasingly recognise the need for organisations to reduce the attack surface they expose to hackers, we can expect increased adoption of similar policies in other industries and



regions," said Ilan Paretsky, Ericom Software's CMO. "With the introduction of clientless remote browser isolation solutions such as Ericom Shield, which is nearly transparent to users and easy to install and manage, there is no reason for organisations to remain vulnerable to browser-borne attacks."

Three main features of Ericom Shield:

- A critical defence with in-depth layer that stops web-borne malware before it reaches endpoints and networks
- Protection against known and unknown malware and ransomware and zero-day threats
- Strong defence against malware in websites, email links and downloaded content SST

Singapore Auxiliary Police Force Tests Out Next-generation Command And Control System

Certis CISCO is rolling out a pilot trial for ARGUS, a next-generation command and control system. Certis CISCO comprises Singapore's largest auxiliary police force and Certis CISCO Aviation Security Officers.

Developed by Certis, ARGUS is a feature-rich, task-based command and control solution that operates as an application in the auxiliary police force's smartphones. It enables Certis CISCO officers to be more efficient and productive by boosting their situational awareness as they carry out their duties.

In addition, it lifts efficiency by streamlining security reporting, tasking, action and monitoring processes into a single platform. At Certis' Integrated Operations Centre, the ARGUS system employs smart data analytics to perform pre-emptive operations control and optimise the allocation of resources to the most critical areas.

Following the pilot, ARGUS will be launched in stages in 2019. SST

MANAGING CYBER THREATS USING THE PARETO PRINCIPLE

►► **By Tony Sager,** Senior Vice President and Chief Evangelist and Shannon McClain, GISF, of The Center for Internet Security

Credit card breaches. Identity theft. Ransomware. Theft of intellectual property. Loss of privacy. Denial of service.

Cyber security threats have become everyday news. For most of us, it's a head-spinning mix of dense technical jargon, conflicting expert opinions, doomsday predictions and market hyperbole.

And here's the really concerning part: the vast majority of cyber security problems that plague us today could be prevented by action, technology and policies that are already known or that exist in the marketplace.

Malicious cyber actors are not magicians wielding unstoppable powers; in truth, most organisations are being overwhelmed by massive numbers of relatively mundane parlour tricks.

It's not that companies aren't aware of these threats or that their technical teams aren't skilled enough. Instead, most are just overwhelmed by what we call the "Fog of More"[1] – more work, problems, regulatory and compliance requirements, conflicting opinions, marketplace noise and unclear or daunting recommendations than anyone can manage.

Conducting a cyber security audit can help organisations understand their technical maturity and preparedness – but where to begin improving?

The Center for Internet Security (CIS) applies the Pareto Principle to cyber security to develop the CIS Controls; a prioritised list of actions that effectively boost one's cyber security posture. The CIS Controls is a free-to-use cyber security document that has been downloaded over 100,000 times.

The Fog Of More

As technologies grow more sophisticated and interconnected, developing an organisational approach to cyber security seems more complicated than ever. DDoSing, phishing, ransomware, data leaks, IT security breaches – how can organisations protect themselves in a perpetually advancing threat landscape? Many organisations start with a cyber security audit to help them understand their current posture. Sometimes these audits are required by regulatory organisations. However, companies that are conducting a cyber security audit – whether to meet compliance, protect digital assets such as intellectual property and trade secrets or to safeguard client/employee information – often run into what CIS calls "the fog of more". This fog surrounds the multitude of problems and solutions facing businesses when it comes to cyber security, obfuscating the task ahead. Most cyber attacks are not the sophisticated, complex activity shown on television and in movies – in fact, attacks often rely on simply misconfigured or outdated systems.

Image: rawpixel on Unsplash.com

Typically, cyber defence is driven by very clever experts dreaming up or demonstrating all of the things that cyber criminals might do, and all of the things that might go wrong. And then they tell you all about the things that you could do to defend yourself.

The CIS Controls focus on what the cyber criminals are doing now, in order to ask "Out of all that I could do, what are the core, foundational steps I can take to get most of my security value and stop these attacks?"

Applying The Pareto Principle

Regardless of industry requirements, it's important to evaluate your organisation's cyber security posture. There is clear evidence that the vast majority of threats out in the wild affect all enterprises, directly or indirectly, whether or not they know it. This means that it is essential for every organisation – regardless of industry, size or function – to take a proactive approach to cyber security.

Once you've conducted an initial cyber security assessment, it's time to start making improvements. You've likely discovered more than a few flaws in your network; unauthorised applications, gaps in incident response plans, or a need for more employee training. Where should you start improving?

In an ever-growing mix of hundreds of potential cyber security concerns and even more proposed solutions, CIS applies the Pareto Principle – the concept that for many activities, roughly 80% of the effects come from 20% of the causes[2] – to help prioritise cyber security actions. For example: in 2002, Microsoft found that roughly 20% of all bugs were causing 80% of reported errors[3]. This discovery allowed them to focus their resources on the most needed fixes.

Focus your efforts on the 20% that will make a difference, instead of wasting time, resources and effort on the 80% that doesn't matter much.[4]

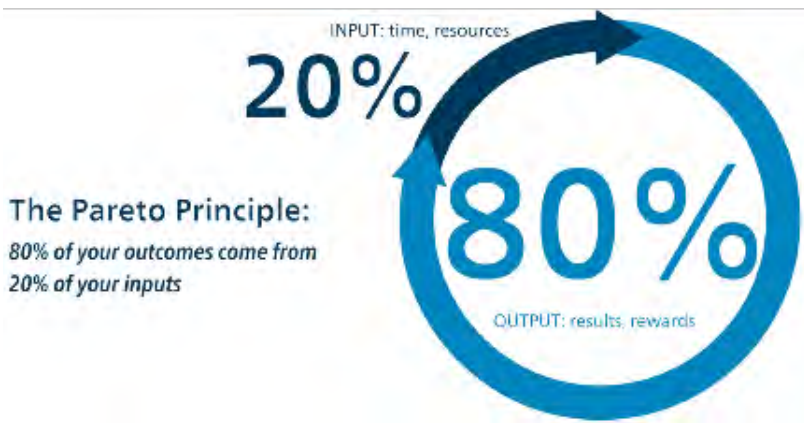
By applying the Pareto Principle to cyber defence actions, CIS has developed the CIS Controls: a set of 20 prioritised actions intended to help any organisation improve its cyber defences. How does CIS narrow down all the possible cyber security actions that an organisation can take?

A Community Approach

Deciding which tasks make the cut isn't a job for just one person or one organisation.

The CIS Controls are developed by a community of cyber security experts around the globe bringing their knowledge and experience with multiple technologies to the table.

Who are these expert volunteers? They come from every part of the cyber ecosystem (companies, governments, individuals); representing every role (threat responders and analysts, technologists, vulnerability finders, tool makers, solution providers, defenders, users, policymakers, auditors); and



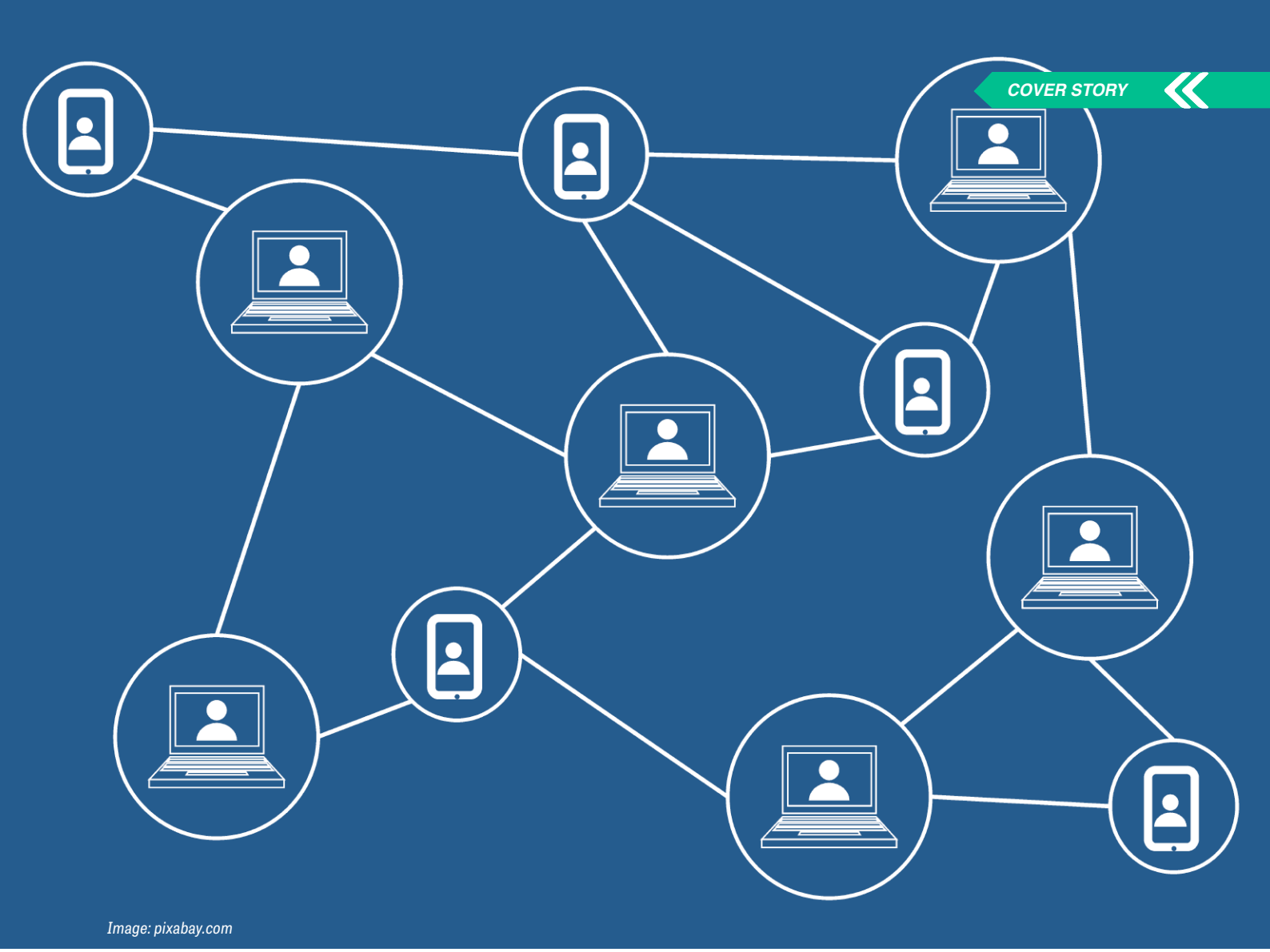


Image: pixabay.com

within many sectors (government, power, defence, finance, transportation, academia, consulting, security, IT). These are people you can't afford to hire, bringing knowledge you don't have, creating content you could not build on your own.

Led by CIS, this community has matured into an international movement of individuals and institutions that:

- Share insight into attacks and attackers, identify root causes, and translate that into classes of defensive action;
- Document stories of adoption and share tools to solve problems;
- Track the evolution of threats, the capabilities of adversaries and current vectors of intrusions;
- Map the CIS Controls to regulatory and compliance frameworks and bring collective priority and focus to them;
- Identify common barriers (like initial assessment and implementation roadmaps) and solve them as a community instead of alone; and
- Make the result of this work available at no cost to any organisation trying to improve its cyber defences.

Their activities ensure that CIS Controls is not just another list of "good things to do", but a prioritised, focused set of actions driven by a community network to make them implementable, usable, scalable and compliant with all industry and government security requirements. The CIS Controls community brings form, structure and prioritisation to the cyber security auditing and remediation process.

Managing Corporate Risk

Keep in mind that any effective cyber security improvement programme should be able to bridge the gap from detailed technical security requirements through basic questions of corporate risk management like:

- Do we know what is connected to our systems and networks?
- Do we know what software is running (or trying to run) on our systems and networks?
- Are we continuously managing our systems using "known good" configurations?
- Are we continuously looking for and managing "known bad" software? Do we minimise and track the people who can bypass, change or override our security defences?
- Are our people aware of the most common threats to our business or mission, and what they can do about them?

These questions aren't rocket science, and most are similar to the kinds of questions that corporate leaders already

ask about physical inventory, safety, finances and other areas of corporate risk management. Each of these questions map directly into one or more of the CIS Controls.

In addition, the CIS Controls map to other popular cyber security regulatory and compliance frameworks including NIST CSF and PCI DSS. As you implement the CIS Controls, you'll be able to track and demonstrate improvements to auditors, vendors, business partners and other cyber security professionals.

First 5 CIS Controls

By using the Pareto Principle to prioritise and organise important cyber security actions, the CIS Controls community has effectively cut through the "Fog of More" to distil the most essential and foundational steps an organisation can take to improve its cyber defence. Below, we'll briefly examine how each of the first 5 CIS Controls can help every organisation bolster its cyber defences and prepare for cyber security audits.

"By using the Pareto Principle to prioritise and organise important cyber security actions, the CIS Controls community has effectively cut through the "Fog of More" to distil the most essential and foundational steps an organisation can take to improve its cyber defence."

CIS Control 1 | Inventory Of Authorised And Unauthorised Devices

This CIS Control helps organisations define a baseline of what must be defended. How can you protect a device unless you're aware of its presence? The inventory process should be as comprehensive as possible and scanners (both active and passive) that can detect devices are the place to start.

In addition to scanning your network for devices, be sure to implement a clear organisational policy to help track and manage devices as they move around the enterprise. Be sure to include company-affiliated cell phones, printers and other network devices.

CIS Control 2 | Inventory Of Authorised And Unauthorised Software

While not a silver bullet for defence, this CIS Control is often considered one of the most effective at preventing and detecting cyber attacks. The purpose of this CIS Control is to ensure that only authorised software is allowed to run on an organisation's systems. While developing an inventory of software is important, application whitelisting is a crucial part of this process, as it restricts the ability to run applications to only those that are explicitly approved.

Implementing CIS Control 2 might mean revisiting company policies and culture; no longer will employees be able to install software whenever and wherever they like. But this CIS Control will likely provide immediate returns to an organisation attempting to prevent and detect cyber attacks.

CIS Control 3 | Secure Configurations For Hardware And Software

By default, most systems are configured for ease of use and not necessarily security. In order to meet CIS Control 3, organisations need to reconfigure systems to a secure standard. Many organisations already have the technology necessary to securely configure systems at scale, such as Microsoft® Active Directory Group Policy Objects and Unix Puppet or Chef.

By utilising configuration standards such as the CIS Benchmarks, most organisations can successfully implement this CIS Control. The consensus-driven CIS Benchmarks is free to download in PDF format for over 150 technologies, including operating systems, middleware and software applications and network devices.

CIS Control 4 | Continuous Vulnerability Assessment And Remediation

The goal of this CIS Control is to understand and remove technical weaknesses that exist in an organisation's information systems. One solution: implement patch management systems that cover both operating system and third-party application vulnerabilities.

Image: pixabay.com

This allows for the automatic, ongoing and proactive installation of updates to address software vulnerabilities. In addition to patch management systems, organisations should implement a commercial vulnerability management system to give themselves the ability to detect and remediate exploitable software weaknesses.

CIS Control 5 | Controlled Use Of Administrative Privileges

This CIS Control ensures that workforce members have only the system rights, privileges and permissions that they need in order to do their job—no more and no less. Unfortunately, for the sake of speed and convenience, many organisations allow staff to have local system or even domain administrator rights. This is too generous and opens the door to abuse, accidental or otherwise. The simple answer is to remove unnecessary system rights or permissions.

Taking The Next Steps

Tackling an organisation's cyber security can often feel intimidating, confusing and just plain daunting but you'll be amazed at what you can achieve by starting with an audit and implementing the most effective strategies first. By working with subject matter experts from around the world and applying a Pareto Principle-informed approach, CIS has helped to bring priority to the world of cyber defence.

Download the CIS Controls document at www.cisecurity.org to access numerous working aids, use cases, resources and a growing user community of volunteers to help you succeed. You'll still have lots of hard work ahead, but the journey becomes manageable with a plan, and with trusted help along the way. SST

---

[1] *https://www.youtube.com/watch?v=OZLO-xekp30*
[2] *http://www.nytimes.com/2008/03/03/business/03juran.html*
[3] *http://www.crn.com/news/security/18821726/microsofts-ceo-80-20-rule-applies-to-bugs-not-justfeatures.*
[4] *http://athinala.com/the-pareto-principle-8020-rule/*

Center for Internet Security, Inc. (CIS®) is a forward-thinking, non-profit entity that harnesses the power of a global IT community to safeguard private and public organisations against cyber threats.

MALWARE: THE KING OF THREATS

Malware has quickly emerged as the king of threats.

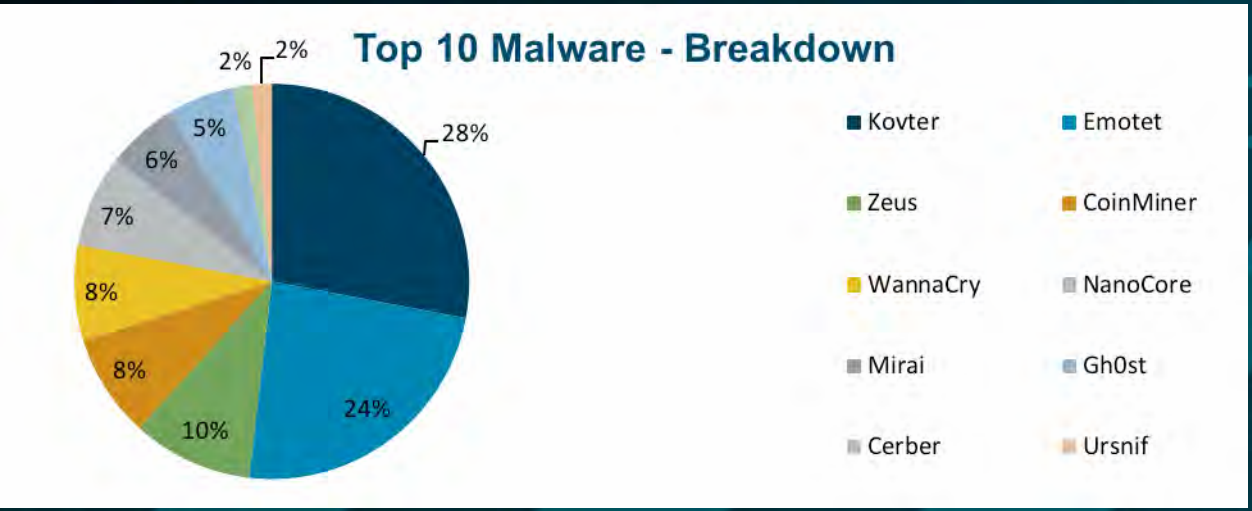
In a recent Bitglass study titled Malware, P.I., nearly half of all organisations were found to be infected, with 44% of organisations revealed to have malware in at least one of their cloud apps.

Bitglass is a global cloud access security broker (CASB) and agentless mobile security company.

What's more, astonishingly few anti-malware tools proved capable of detecting ShurLockr, a new zero-day ransomware. Google Drive, Microsoft SharePoint and 93% of antivirus engines were unable to detect ShurLockr.

So far in 2018, ransomware like WannaCry have continued to spread, and Emotet has emerged as a leading, modular banking Trojan. Cloud cryptojacking is also on the rise.

Security experts are particularly concerned about the evolution of context-aware threats like the Rakhni Trojan, as well as the growth of ransomware-as-a-service. A context-aware threat installs malware best suited for the systems that it is infecting. For example, in computers that have cryptocurrency wallets already installed, Rakhni will deploy ransomware that encrypts the device and requires victims to pay a cryptocurrency ransom for decryption. Ransomware-as-a-service is where hackers offer ransomware platforms that inexperienced cyber criminals can use to hold data hostage. SST



Top 10 Malware August 2018 | By Center for Internet Security

In August, Malspam continues to dominate as the primary infection vector with half of the top 10 malware being delivered by this method. Malware in the Top 10 Malware list continue not to use malvertisement as a delivery mechanism.

The top 10 malwares in August 2018 are:

#1 Kovter. This is a fileless click fraud malware and downloader that evades detection by hiding in registry keys. Reports indicate that Kovter can have backdoor capabilities and uses hooks within certain APIs for persistence.

#2 Emotet. This modular infostealer downloads or drops banking Trojans. It can be delivered through either malicious download links or attachments such as PDFs or macro-enabled Word documents. Emotet also incorporates spreader modules in order to propagate throughout a network.

#3 ZeuS. This modular banking Trojan uses keystroke logging to compromise victim credentials when the user visits a banking website. Since the release of the ZeuS source code in 2011, many other malware variants have adopted parts of its codebase, which means that events classified as ZeuS may actually be other malware using parts of the ZeuS code.

#4 CoinMiner. This cryptocurrency miner uses Windows Management Instrumentation (WMI) and EternalBlue to spread across a network. CoinMiner uses the WMI Standard Event Consumer scripting to execute scripts for persistence.

#5 WannaCry. This ransomware cryptoworm uses the EternalBlue exploit to spread via SMB. Version 1.0 has a "killswitch" domain, which stops the encryption process.

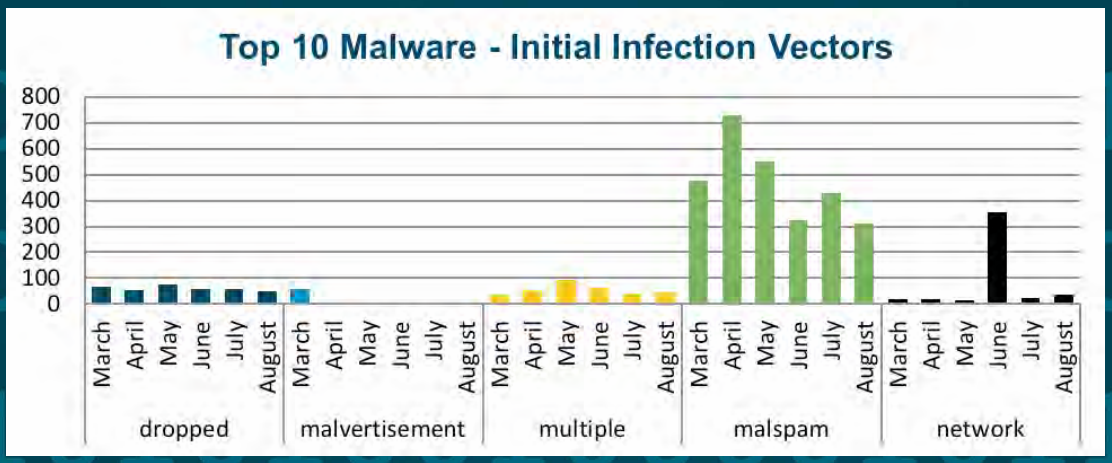
#6 NanoCore. This Remote Access Trojan (RAT) spreads via malspam as a malicious Excel XLS spreadsheet. As a RAT, NanoCore can accept commands to download and execute files, visit websites and add registry keys for persistence.

#7 Mirai. This malware botnet is known to compromise Internet of Things (IoT) devices in order to conduct large-scale distributed denial of service (DDoS) attacks. Mirai is dropped after an exploit has allowed the attacker to gain access to a machine.

#8 Ghost. This RAT is used to control infected endpoints. Ghost is dropped by other malware to create a backdoor into a device that allows an attacker to fully control the infected device.

#9 Cerber. This is an evasive ransomware capable of encrypting files in offline mode and is known for fully renaming files and appending them with a random extension. There are currently six versions of Cerber evolved specifically to evade detection by machine learning algorithms. Currently, v1 is the only version of Cerber for which a decryptor tool is available.

#10 Ursnif, and its variant Dreambot, are banking Trojans known for weaponising documents. Ursnif recently upgraded its web injection attacks to include TLS callbacks in order to obfuscate against anti-malware software. Ursnif collects victim information from login pages and web forms.



The MS-ISAC Top 10 Malware refers to the top 10 new actionable event notifications of non-generic malware signatures sent out by the MS-ISAC Security Operations Center (SOC).

Dropped – Malware delivered by other malware already on the system, an exploit kit, infected third-party software, or manually by a cyber threat actor.
Malvertisement – Malware introduced through a malicious advertisement.
Multiple – Refers to malware that currently favours at least two vectors.
Malspam – Unsolicited emails, which either direct users to download malware from malicious websites or trick the user into opening malware through an attachment.
Network – Malware introduced through the abuse of legitimate network protocols or tools such as SMB or remote PowerShell.

Center for Internet Security, Inc. (CIS®) is a forward-thinking, non-profit entity that harnesses the power of a global IT community to safeguard private and public organisations against cyber threats.

Image: Pixabay.com

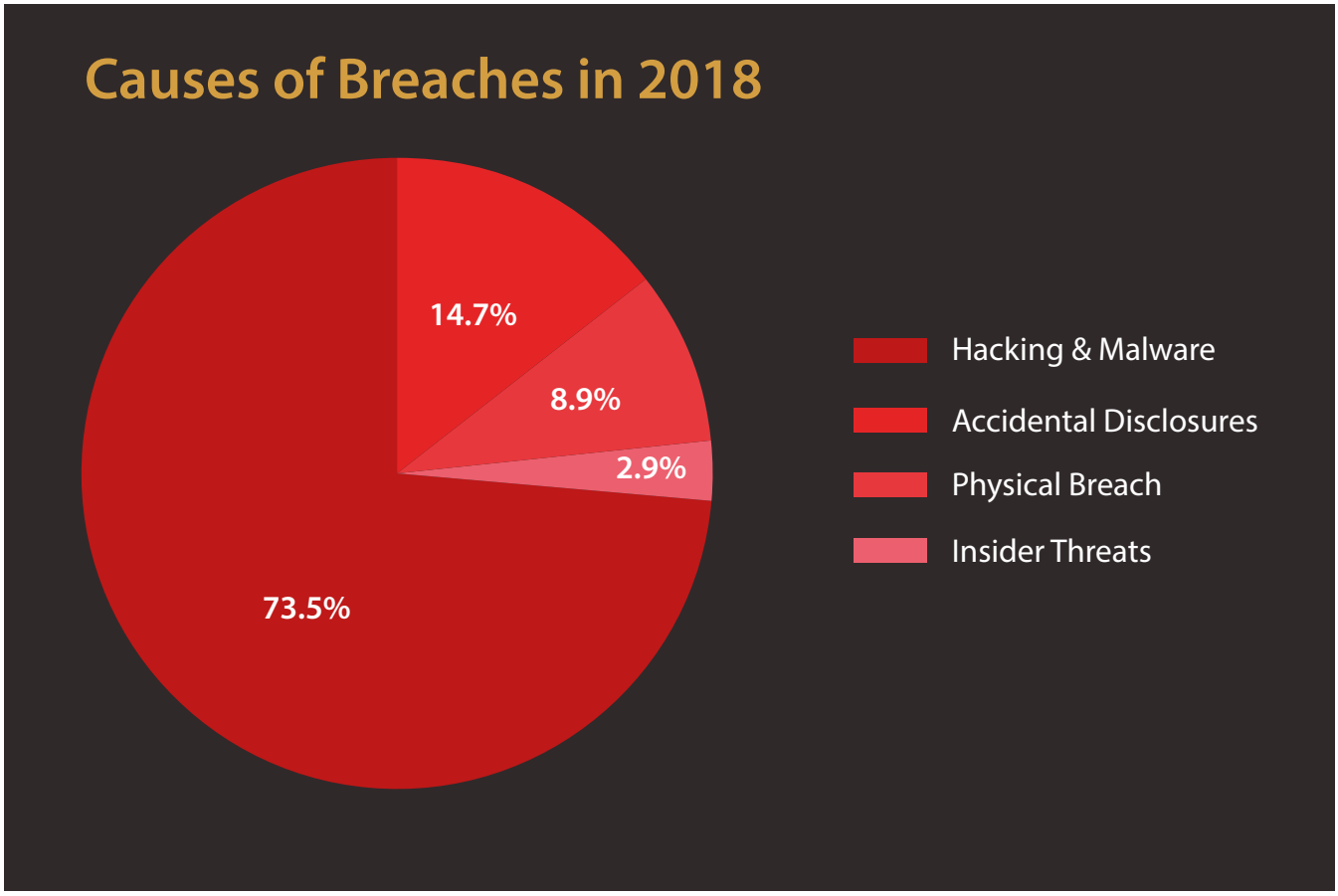
2018: A Threatening Year For Financial Services

The financial sector was hit hard by cyber attacks in 2018.

According to the 2018 Financial Breach Report by Bitglass, 2018 has been far more dangerous than 2016, the last year that Bitglass conducted a financial breach report.

In 2018, there were nearly three times as many breaches as there were two years ago. This is largely due to the explosive growth of hacking and malware around the world, detailed the Next-gen CASB (Cloud Access Security Broker) company. And many of these were aimed squarely at financial services.

"Financial organisations regularly handle sensitive, regulated data like home addresses, bank statements and Social Security numbers," said Rich Campagna, CMO of Bitglass. "This type of information is an incredibly attractive target for criminals, meaning financial services firms need to be highly vigilant when it comes to cyber security. Failing to protect data and reach regulatory compliance can spell disaster for any company." For this report, Bitglass aggregated data from the Identity Theft Resource Center and the Privacy Rights Clearinghouse.



From January to August of 2018, financial services firms experienced 103 breaches, compared to the 37 recorded over the same time frame in 2016.

Not only were there more breaches, the breaches caused far more damage.

The top three breaches in 2018 were SunTrust Banks (1.5 million records exposed) Guaranteed Rate (188,000 records exposed), and RBC Royal Bank (66,000 records exposed). In 2016, the sum total of all breached records was 64,512.

In the case of SunTrust Banks, a former employee of SunTrust Banks stole (and possibly shared) 1.5 million customers' names, addresses, phone numbers and account balances.

As for RBC Royal Bank, an unauthorised party accessed the bank's Travelocity platform and stole the payment card information of 66,000 users of RBC's Travel Rewards website.

The increase in breaches is likely due to a large number of reasons, indicated Bitglass. Some organisations may be overly reliant on existing cyber security infrastructure and find it difficult to justify additional expenses in light of their existing sunk costs in security. Other firms may simply overrate what traditional endpoint and premises-based tools can do to protect data from evolving threats.

A Full Onslaught Of Hacking And Malware

Hacking and malware were responsible for nearly three quarters of all breaches in 2018. This is a massive increase over previous years, where they were responsible for 20% of breaches.

Noteworthy threats to financial firms in 2018 include cloud cryptojacking, ransomware-as-a-service platforms, modular banking trojans like Emotet and ransomware like WannaCry.

With malware continuing to spread and evolve, the financial services sector should be very concerned about it, stated Bitglass. "It is now clear that defending against malware deserves special attention. This is particularly true in light of the rise of cloud and BYOD. More devices and applications are storing and processing data than ever before, creating more opportunities for malware to infect the enterprise."

The sector can do far more to secure sensitive information, Bitglass advocated. SST

DISTRUST OF EPAYMENT AND POOR CYBER HYGIENE IN SINGAPORE

Nearly half (45%) of Singaporeans surveyed - the highest in Southeast Asia - do not take proper measures to secure their financial data and use the same passwords for some to all of the services and apps that contain their personal payment data.

This was revealed in the recently released VMware Banking Consumer 2020 study. This is a regional multi-country study conducted in September 2018 that surveyed the behaviours, preferences and attitudes towards banking and the future of payments of 6,000 consumers in

Sanjay K. Deshmukh, Vice President and Managing Director, Southeast Asia and Korea, VMware

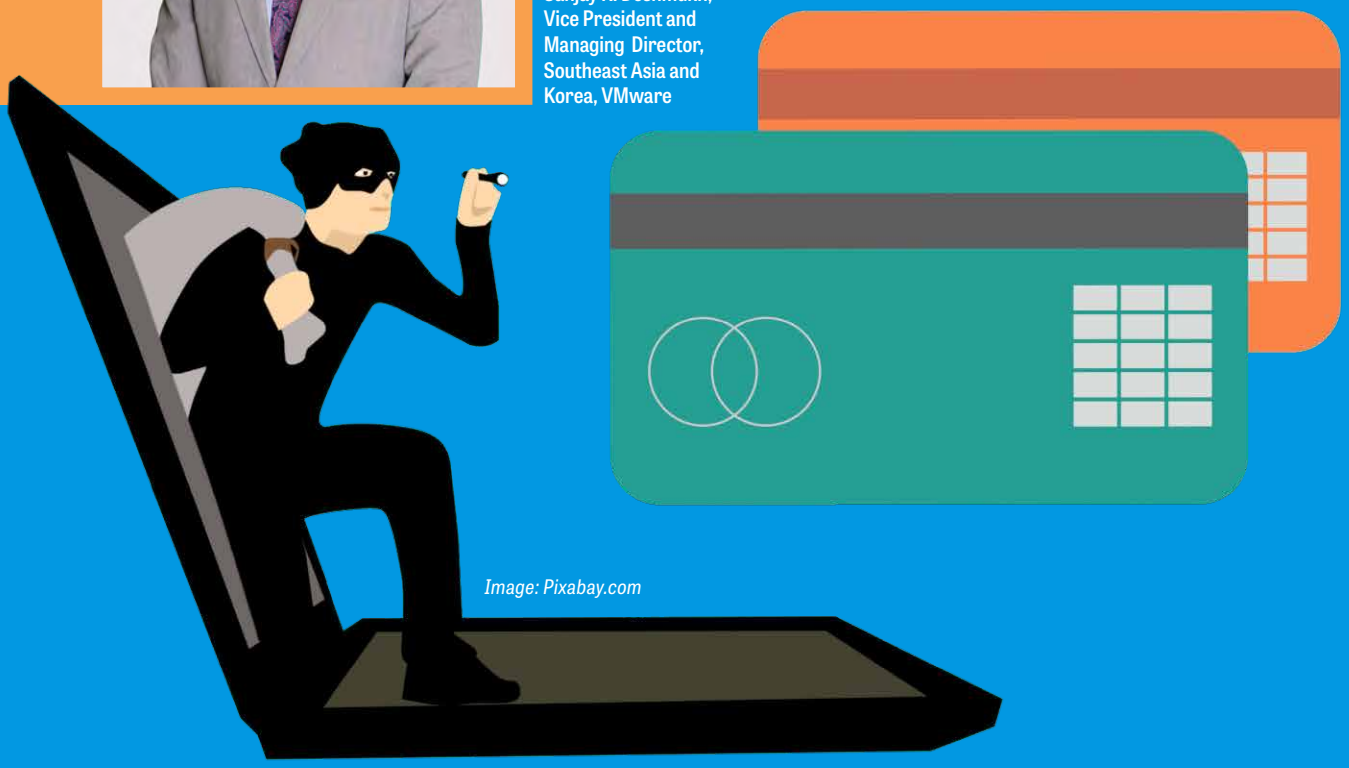


Image: Pixabay.com

Indonesia, Malaysia, Singapore, the Philippines, Thailand and South Korea. VMware, Inc. is a leading innovator in enterprise software.

An astonishing 76% of Singapore consumers surveyed store their bank account details on at least one to six applications, yet only a handful (14%) are practicing good cyber security practices by using different passwords for all their accounts, making Singapore the country with the least cyber hygiene of those surveyed in the region. Thailand takes the lead at 30%.

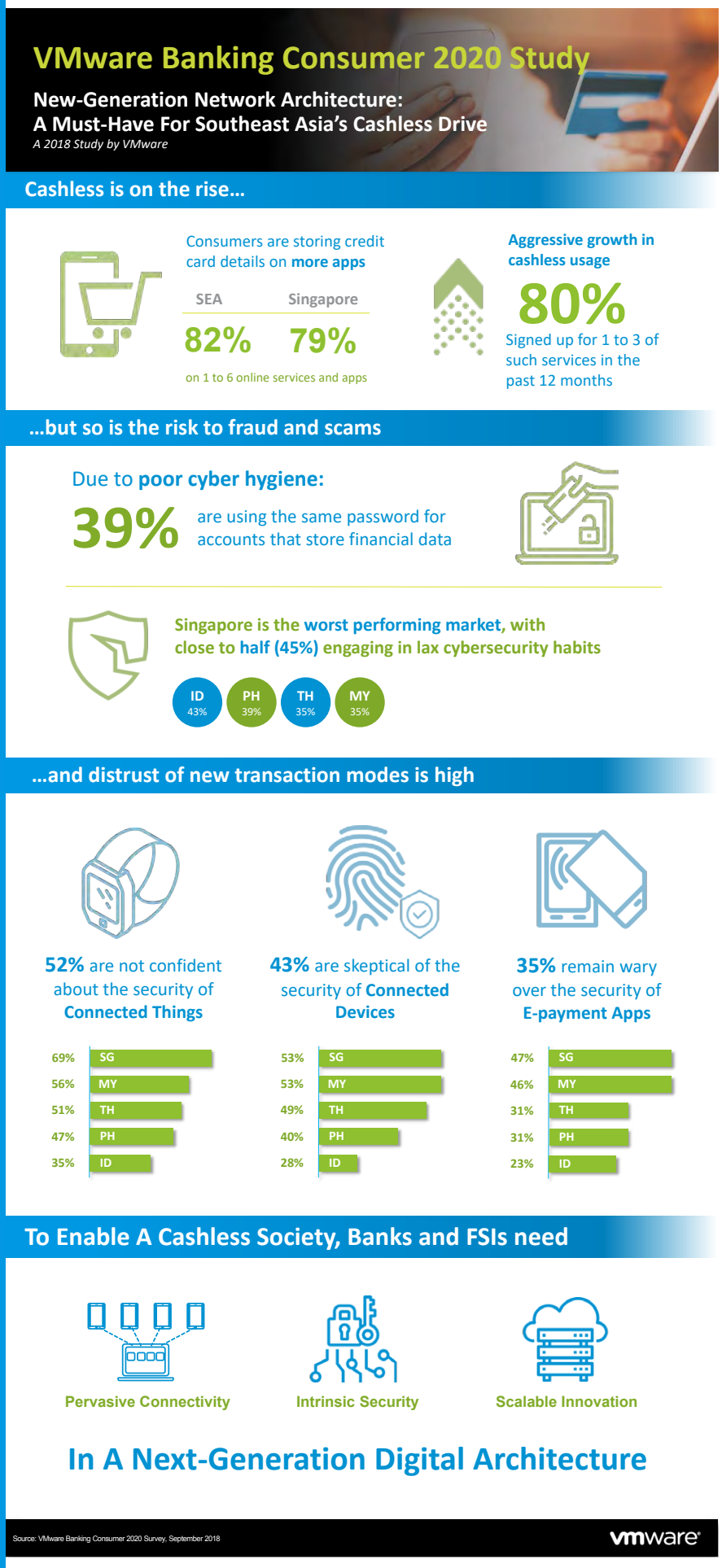
While the increasing uptake in cashless payments is an encouraging sign for Singapore's cashless ambitions, poor cyber hygiene practices could put consumers, banks and financial institutions at greater risk of financial fraud and losses.

"With Singapore expected to be 82% cashless by 2022, according to Frost & Sullivan's Future of Cashless Payment in Singapore 2018 report[1], banks and financial institutions (FSIs) have a pressing need to boost their cyber security defences," said Sanjay K. Deshmukh, Vice President and Managing Director, Southeast Asia and Korea, VMware. "Existing architecture is insufficient to guard against this new payment reality – banks and FSIs need a new network infrastructure to protect their apps, data and users across multiple cloud environments."

Singaporeans Distrust ePayment

The study also found that Singapore consumers are more sceptical about the level of security afforded by new payment methods than their counterparts in other countries in the region, preferring the security of traditional payment methods such as cash and ATMs.

In contrast, consumers in Indonesia, the Philippines and Thailand place greater trust in connected things as new methods of payment.



Banks and FSIs face increased scrutiny over how personal data is handled and an unyielding demand for fast response to consumers. Finding the right balance between staying attuned to consumers' needs in compliance and security, while future-proofing their digital foundation with innovation can be tricky but critical, especially when we are turning to technologies of the future.

Image: Pixabay.com

Banks And FSIs Can Do Better

What this means is that banks and FSIs need to do more to give consumers in Singapore peace of mind.

Singapore consumers also indicated areas of improvement for banks to do better in, rating these attributes lower than the regional average:

- Transparency in policies and understandable terms and conditions;
- Data privacy security and ethical use of personal data;
- Speed in answering queries or resolving issues;
- Availability of customer service channels.

In order to further secure online payment platforms, banks and FSIs continue to innovate to meet the shifting demands of mobile-first consumers. Forward-thinking banks are already gaining traction with the introduction of biometric payment. At least three quarters of consumers in the region place high trust in the technology, alongside cash payment.

"Banks and FSIs face increased scrutiny over how personal data is handled and an unyielding demand for fast response to consumers. Finding the right balance between staying attuned to consumers' needs in compliance and security, while future-proofing their digital foundation with innovation can be tricky but critical, especially when we are turning to technologies of the future," commented Deshmukh.

Deshmukh recommends a Virtual Cloud Network architecture that harnesses the power of networking technologies. This will empower banks and FSIs to respond faster to new opportunities and threats, create new business models, and deliver services to all applications and data, wherever they are located.

He explained. "As cities in the region embark on their journey to becoming smart cities and nations with next-generation technologies, establishing a highly secured infrastructure will be mission-critical for verticals such as banks and FSIs."

Innovation needs to rest on a robust network architecture built on speed, intelligence and 'zero trust', urges VMware.

[1] *Frost & Sullivan, Future of Cashless Payment in Singapore 2018, 2018*

VMware Banking Consumer 2020 Study: A Snapshot

How many online services, apps, or subscriptions do you store bank, debit or credit card details on?

- Southeast Asia:
  1. 58% store them on between 1 – 3 apps or services
  2. 25% store them on between 4 – 6 apps or services
  3. 17% store them on 7 or more apps or services
- Singapore:
  1. 46% store them on between 1 – 3 apps or services
  2. 30% store them on between 4 – 6 apps or services
  3. 24% store them on 7 or more apps or services
- Indonesia:
  1. 65% store them on between 1 – 3 apps or services
  2. 22% store them on between 4 – 6 apps or services
  3. 13% store them on 7 or more apps or services
- Malaysia:
  1. 52% store them on between 1 – 3 apps or services
  2. 30% store them on between 4 – 6 apps or services
  3. 18% store them on 7 or more apps or services
- Philippines:
  1. 62% store them on between 1 – 3 apps or services
  2. 22% store them on between 4 – 6 apps or services
  3. 16% store them on 7 or more apps or services
- Thailand:
  1. 63% store them on between 1 – 3 apps or services
  2. 23% store them on between 4 – 6 apps or services
  3. 14% store them on 7 or more apps or services

Do you use the same password and login across some to all of your online accounts? (% of consumers using the same password and login across some to all of their online accounts)

- Southeast Asia: 39%
- Singapore: 45%
- Indonesia: 43%
- Malaysia: 35%
- Philippines: 39%
- Thailand: 35%

Do you use different passwords and logins for all of your online accounts? (% of consumers using different passwords and logins for all online accounts)

- Southeast Asia: 24%
- Singapore: 14%
- Indonesia: 25%
- Malaysia: 25%
- Philippines: 28%
- Thailand: 30%

How secure do you think the following transaction methods are? (On a scale of 1 – 10, 1 being the least secure and 10 the most secure, % of consumers indicating 7 to 10)

a) Biometric identification (e.g. fingerprint, iris scans):
- Southeast Asia: 78%
- Singapore: 72%
- Indonesia: 85%
- Malaysia: 71%
- Philippines: 81%
- Thailand: 79%

b) Connected things (e.g. fashion accessory, wireless speaker with payment capabilities):
- Southeast Asia: 48%
- Singapore: 31%
- Indonesia: 65%
- Malaysia: 44%
- Philippines: 53%
- Thailand: 49%

c) Connected devices (e.g. smart watches, mobile phone with wallets such as ApplePay):
- Southeast Asia: 57%
- Singapore: 47%
- Indonesia: 72%
- Malaysia: 47%
- Philippines: 60%
- Thailand: 60%

d) E-payment wallets and apps:
- Southeast Asia: 65%
- Singapore: 53%
- Indonesia: 77%
- Malaysia: 54%
- Philippines: 69%
- Thailand: 69%

e) Mobile apps from banks:
- Southeast Asia: 71%
- Singapore: 65%
- Indonesia: 80%
- Malaysia: 66%
- Philippines: 70%
- Thailand: 74%

f) Online interbank transfer:
- Southeast Asia: 76%
- Singapore: 73%
- Indonesia: 85%
- Malaysia: 71%
- Philippines: 75%
- Thailand: 75%

g) ATMs:
- Southeast Asia: 77%
- Singapore: 78%
- Indonesia: 85%
- Malaysia: 71%
- Philippines: 79%
- Thailand: 73%

How comfortable are you with using a digital-only bank (i.e. a bank that does not have a physical presence and is 100% online)? (On a scale of 1 – 10, 1 being the least comfortable and 10 the most comfortable, % of consumers indicating 7 to 10)

- Southeast Asia 59%
- Singapore: 42%
- Indonesia: 74%
- Malaysia: 47%
- Philippines: 60%
- Thailand: 69%

THE 5 ESSENTIAL ELEMENTS OF A SUCCESSFUL SOFTWARE SECURITY INITIATIVE

▸▸ **By Olli Jarva,** Managing Consultant, Asia Pacific, Synopsys Inc.

Image: Pixabay.com

A year or two ago, minimal effort on software security may have been sufficient to prevent your organisation from being attacked and breached. Today, if you don't have someone (or a team) specifically responsible for software, application or product security, you are falling further behind every minute and regulators, attackers, customers and executives are noticing.

Every organisation that develops or integrates software as a core part of their business needs a software security initiative — a blend of people, processes and tools that ensures applications and the data they process are secure. As customers, regulators, executives and boards of directors start asking for evidence of a formal approach to software security, organisations are trying to determine where to start, how to construct a viable initiative, and what people, processes and technologies they will require.

Fortunately, you can jumpstart this process immediately and quickly build the foundation for a software security initiative that will satisfy your security needs today and in the future. There are innovative ways to rapidly establish a functional and scalable software security initiative that results in secure, higher quality software at a significantly lower cost and level of effort.

The key is to plan and implement the initiative in stages, focusing on highest risks first, while building in the flexibility to scale and adapt the initiative to address your evolving technical and compliance requirements.

When effectively implemented, a software security initiative results in:

- Executives who understand its value and impact
- A software security group that is able to govern
- Security teams that are integrated into the development processes
- Internal and external stakeholders that accept the initiative as compliant with their risk tolerance
- A grasp of good software security practices

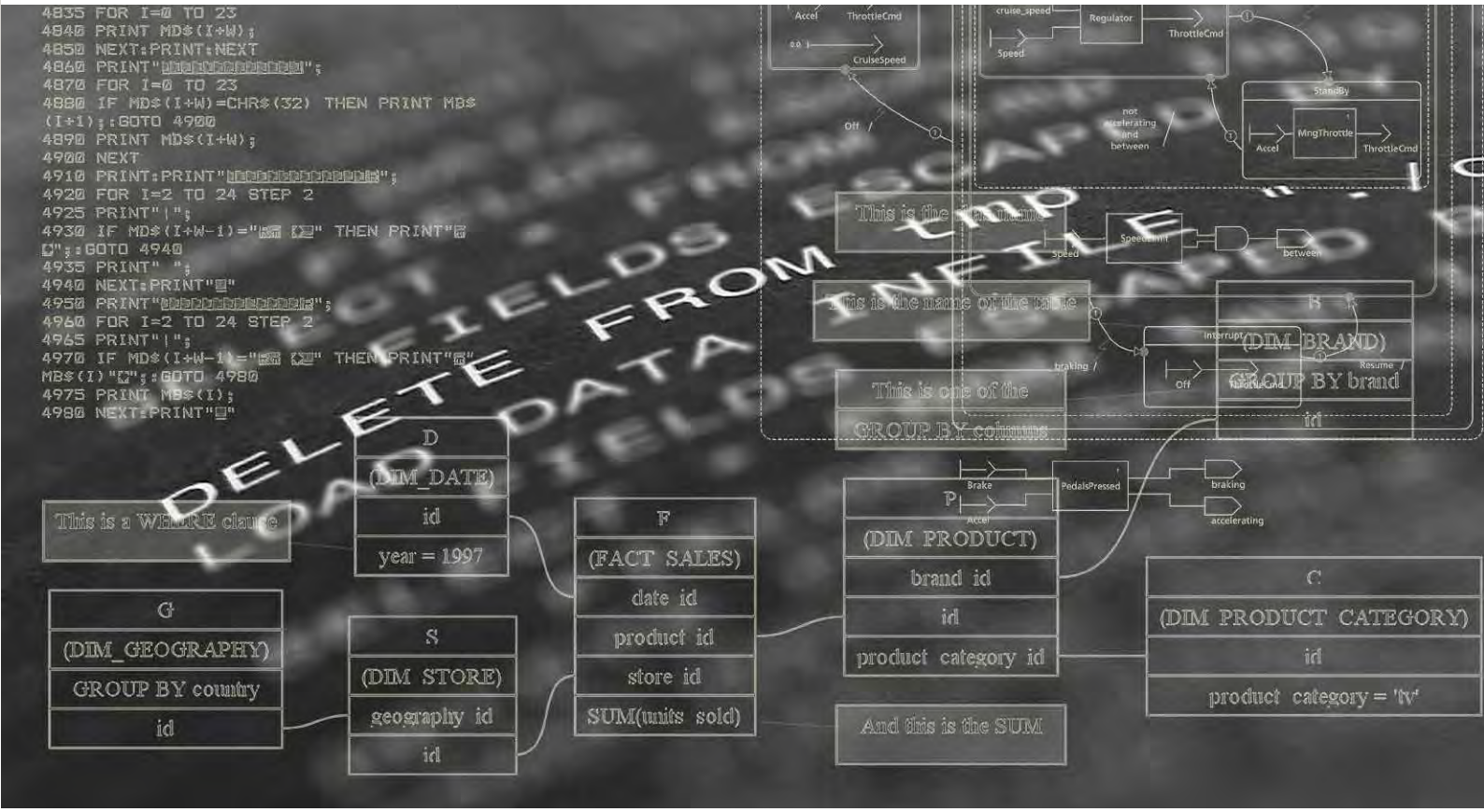
Yes, You Will Be Tested

Pressure to build and implement software more securely is mounting for all firms. This encompasses everything from commercial software and back-end servers to embedded components and devices connected to the Internet of Things (IoT).

Applications are one of the top targets for attacks and yet few organisations have the resources, skills or technical expertise to find, fix and prevent security vulnerabilities.

Soon, however, your software security posture will be tested - whether you pay someone to or not.

External and internal forces will surface to test your security posture. Government agencies, compliance regulators, customer auditors and your own executives will ask how you manage software security risks. The Federal Trade Commission announcing consent decrees enforcing data security regulations and the Payment Card Industry Security Standards Council



regulating and enforcing PCI DSS compliance are but two examples of external forces announcing their intention to drive software security improvements industry wide.

In addition, when data of varying sensitivity levels is spread across tens or hundreds of enterprise systems, the burden to demonstrate compliance during an audit quickly becomes daunting. Regardless of which regulatory and compliance standards your organisation must adhere to, someone will be asking you questions about your ability to create, deploy and maintain secure software.

Hackers and other malicious actors will test your security posture. Maybe your organisation hasn't been breached yet, or worse, maybe you have been breached but haven't yet discovered the intrusion. Either way, chances are your organisation will be attacked and may suffer a breach at some point.

Enterprise customers will also start to test your security posture. As part of an increasingly common risk management strategy, organisations that license your applications or integrate your software into their enterprise applications and environments will require you to demonstrate the existence of a software security initiative as part of the vendor selection and management process.

This will become common in requests for proposal, license negotiations, M&A due diligence and other facets of business-to-business (B2B) and business-to-consumer (B2C) interactions. As more organisations realise the security risks they inherit from other companies through the software supply chain, they will demand evidence of an effective software security initiative because simply accepting the risk associated with insecure software is no longer an option.

Tests of your organisation's security posture will also come from senior executives and the board of directors. They will demand to know what you are doing to keep the company from becoming the next breach victim. They will want to understand the details of the software security initiative you have in place to keep them from being fired or ending up in jail.

The bottom line: Many different stakeholders, agencies and threats are creating pressure to build your software more securely. Given the limited impact and effectiveness of disjointed security activities, this confluence of macro and micro trends and events makes a focused, holistic initiative for software security a necessity.

The 5 Essential Elements Of A Successful Software Security Initiative

There is no single product, service or SaaS offering that will solve your software security problems. No static security testing tool or penetration test alone will solve the problem. No threat intelligence service that can put security into software. Network scanning tools don't address the problem. Each of these approaches provides visibility into isolated aspects of the problem but does not deliver an actual solution. They are all important components of the solution, but used in isolation as part of a piecemeal approach, none of these products, portals, services or tools will actually help you improve your security posture.

Without a software security initiative, you're not optimising your security investments or outcomes.

The goal of establishing a software security initiative is to improve the security of all deployed software — whether acquired, outsourced, used as a service or developed internally — through a disciplined and scalable approach. At its most basic, your initiative is a combination of people dedicated to software security (commonly referred to as a Software Security Group) and the processes and technologies they employ to ensure your applications are not exposed to unacceptable levels of risk.

There is no one-size-fits-all product or initiative. Each organisation needs to map out a strategy, establish best practices and plan for a right-sized initiative and level of effort that meets its software security needs. Building a software security initiative does not need to be an overly complex, time-consuming or expensive process. In fact, there are only five key characteristics your initiative must have in order to quickly deliver meaningful and visible improvements in your software security posture.

"The goal of establishing a software security initiative is to improve the security of all deployed software — whether acquired, outsourced, used as a service or developed internally — through a disciplined and scalable approach. At its most basic, your initiative is a combination of people dedicated to software security (commonly referred to as a Software Security Group) and the processes and technologies they employ to ensure your applications are not exposed to unacceptable levels of risk."

Your software security initiative must include:

1. A dedicated Software Security Group of at least one person

To ensure the success of your software security initiative, it is imperative that you remove resource constraints and provide the infrastructure and capabilities for staff to effectively support your initiative. If you can clearly demonstrate value through policies, processes and a charter, even a one-person Software Security Group can evolve into a fully supported team.

2. A software security policy

It is important to lay out the software security policy statements that define the business controls that manage risk across your software portfolio. A software security policy can cover areas such as application risk ranking, development project impact ranking and data classification. These policy statements should also clarify mandatory objectives and describe what each stakeholder must accomplish.

3. Security tools for your developers

Drive efficiencies by helping developers fix security defects before they are committed to the code base. This will prevent common vulnerabilities from ever being introduced. Enabling developers to fix defects in real-time is less expensive than scanning completed applications for defects and entering a fix-and-retest cycle. Early detection and remediation may remove potential delays in releases and prevent patch cycles, eliminating the significant costs associated with each. An effective approach is leveraging an IDE plug-in that automatically provides "just in time" security guidance as the code is written. It empowers developers to create secure code the first time with a tool that acts as a desktop security expert, providing guidance automatically.

4. Training for internal and external development teams

Provide software security awareness and best practices across your organisation through an on-demand training e-library. This enables your firm to scale knowledge transfer efforts and ensures developers are exposed to secure coding practices.

5. Reports to validate progress and value to executives

Proactively and consistently provide your senior management with greater visibility into and governance over the business risk associated with your organisation's software assets. Showing progress from baselines toward objectives is critical if you want to maintain (or increase) ongoing support and resources for your software security initiative.

In A Nutshell

Building a software security initiative can be intimidating, but there are experts available to streamline the process of building an initiative that can grow and adapt to your evolving software security requirements. The pressure to implement a more focused and holistic initiative around software security is coming from many directions - from customers and senior executives to regulatory agencies and the companies in your software supply chain. For all these stakeholders, accepting the risks of insecure software is no longer an option. Piecemeal products and services will not reliably improve your security posture. The cost-effective solution is a software security initiative that integrates all the individual policies, tools and processes. SST

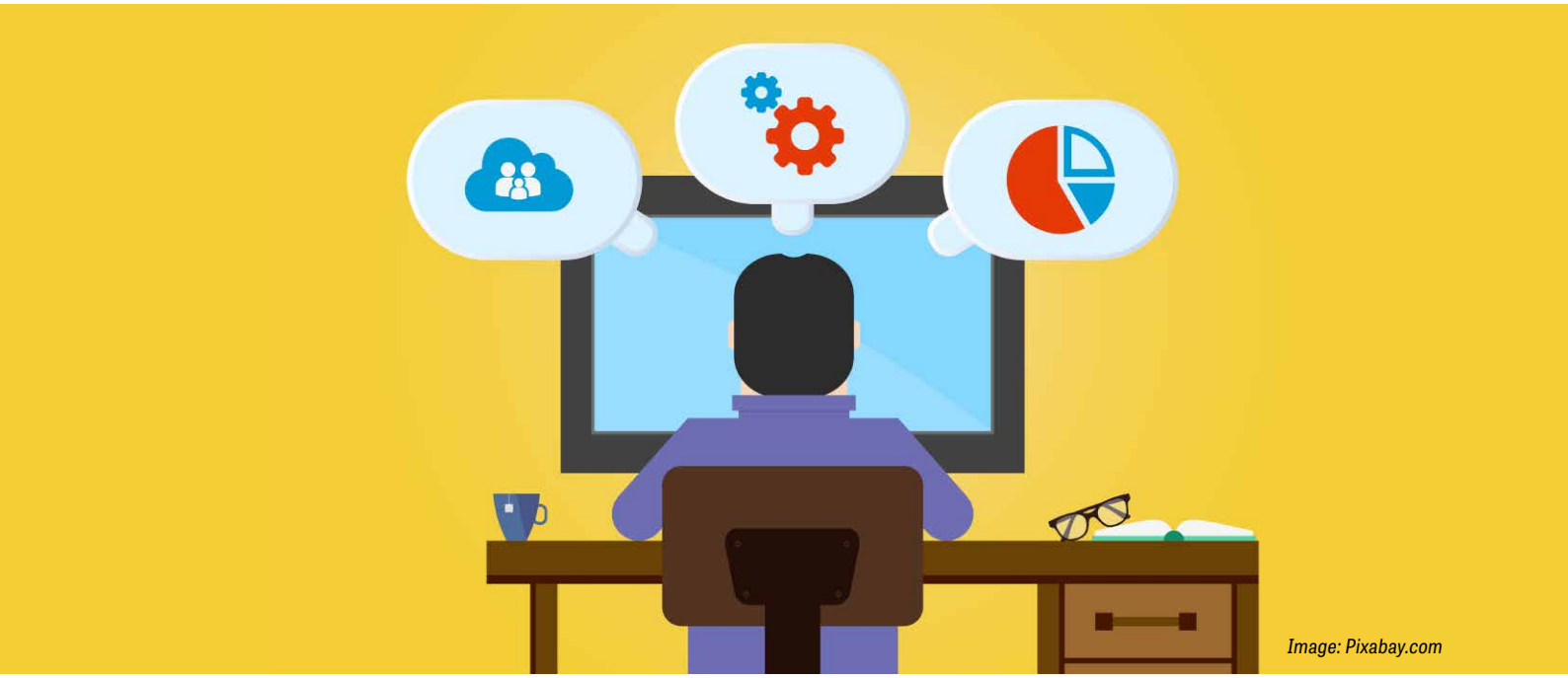


Image: Pixabay.com

PREVENTING RANSOMWARE RISKS: 5 CRITICAL TIPS

▸▸ By Check Point Technologies Research Team

At an annual price tag of around US$11.5 billion*, ransomware is big business for criminals and a big headache for business. Whether it's an entire major US city or a small mom-and-pop company, cyber attackers are unleashing ransomware on enterprises and organisations of all sizes.

In the fight against ransomware, the best strategy is to not become a victim in the first place. But where can you begin? The following best practices can help you prevent ransomware attacks against your organisation.

Back Up Your Data And Files Regularly

With the advent of more reliable networks and cloud-based storage, many of us have simply gotten out of the habit of backing up files and data. However, in the event of a ransomware attack, it may be possible to use these backups in lieu of paying the ransom. At the very least, they will allow you to decide for yourself whether the cost of restoring from backup is more or less costly than the requested ransom.

There is also a second reason why it is extremely important to have those backups. Even if you are willing to pay the ransom, keep in mind that you are placing your trust in the hands of cyber criminals. How confident are you that they will actually provide you the decryption key once you pay? Or even worse, you pay, they give you a key, and you still can't recover your files. The ransomware may have bugs, or may not work in your environment. Keep in mind that ransomware is not commercial software that has been run through rigorous quality assurance testing.

Since it is not wise to place trust in your attacker, it is important that you consistently back up your important files, preferably using air-gapped storage. Enable automatic backups, if possible, for your employees, so you don't have to rely on them to remember to execute regular backups on their own.

Constantly Educate Employees To Recognise Potential Threats

User education has always been key to avoiding malware infection. This same principle also applies to ransomware. The basics of knowing where files came from, why the employee is receiving them, and whether or not they can trust the sender are useful know-how your employees should draw on before opening files and emails.

The most common infection methods used in ransomware campaigns are still spam and phishing emails. Quite often, user awareness can prevent an attack before it occurs. Take the time to educate your users, and ensure that if they see something unusual, they report it to your security teams immediately.

Limit Access To Those Who Need It Through Segmentation and User Permissions

In order to minimise the potential impact of a successful ransomware attack against your organisation, ensure that user permissions in your organisation are set up correctly for individual users, so that they only have access to the information and resources they require to perform their work. This reduces the likelihood of malicious files being executed. Another important factor is to implement network segmentation. Taking this step significantly reduces the possibility of a ransomware attack moving laterally throughout your network. Addressing a ransomware attack on one user system may be a hassle, but the potential implications of a network-wide attack can be dramatically greater.

Keep Up To Date With Your Patches And Security Signature

From an information security perspective, it is beneficial to keep antivirus and other signature-based protections in place and up to date. While signature-based protections alone are not sufficient to detect and prevent sophisticated ransomware attacks designed to evade traditional protections, they are an important component of a comprehensive security posture. Up-to-date antivirus protections can safeguard your organisation against known malware that has been seen before and that has an existing and recognised signature.

Implement Multi-layered Security That Deals With Advanced Threats

They say that the best defence is a good offense, and implementing a multi-layered approach to security provides the best opportunity to fend off ransomware and the damage that it can cause. In addition to traditional, signature-based protections like antivirus and IPS, organisations need to incorporate additional layers to counter new, unknown malware that has no known signature. Two key components to consider are threat extraction (file sanitisation) and threat emulation (advanced sandboxing). Each element provides distinct protection, that when used together, offer a comprehensive solution for protection against unknown malware at the network level and direct protection on endpoint devices.

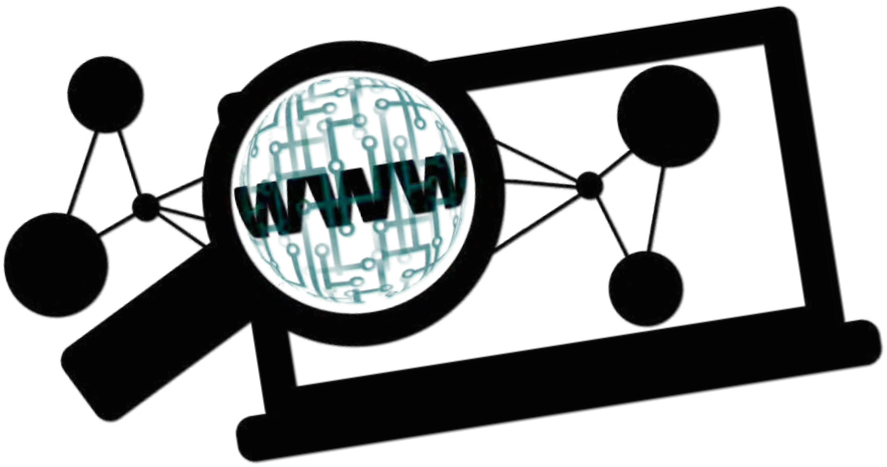
To sum up, implementing a few key preventative measures in the fight against ransomware can be the difference between staying safe and becoming a victim. Always back up your data to ensure you have it available in the event your files are encrypted. Educate your employees to recognise and avoid potential threats, and limit their access to only those systems and files that they actually need in order to carry out their work. Keep your antivirus and other signature-based protections up to date to prevent the preventable. And implement advanced threat prevention solutions as part of a multi-layered approach to security to prevent unknown attacks, like ransomware, against your organisation. SST

Image: Pixabay.com

**source: https://www.cybereason.com/blog/how-much-does-a-ransomware-attack-cost*

IT Professionals in Asia Find Web And Mobile Apps Challenging To Secure

Images: Pixabay.com



A 2018 survey by Synopsys of 251 IT professionals revealed that customer-facing web applications continue to present the highest security risk to businesses in Asia Pacific (36% of the respondents), followed by internal-facing web applications (26%) and mobile applications (25%).

The survey was conducted at GovernmentWare (GovWare) 2018, the anchor conference of cyber security convention Singapore International Cyber Week 2018. The in-person survey is based on responses from attendees including C-Suite IT professionals as well as managers and other executives.

The survey covered a broad spectrum of important areas, including cyber security and incident response strategies, types of applications at risk, availability of skilled cyber security personnel at the workplace, training and development and open source adoption approaches.

The good news is that 71% of respondents said they have an incident response plan in place in the event of a security incident, an increase over 2017. The bad news is that despite the rise in Open Source Software (OSS) adoption, 30% of the organisations surveyed do not have an inventory management process for OSS.

This is the second consecutive year that IT professionals in Asia report that they are struggling with securing web and mobile applications.

"It is not surprising that web and mobile applications continue to pose such a major challenge to businesses in the Asia Pacific region," commented Geok Cheng Tan, managing director of Asia Pacific at the Synopsys Software Integrity Group, "as these applications often process highly sensitive information and cyber attacks targeting them are growing in sophistication. With an escalating number of cyber security incidents large and small, it is increasingly clear that software development life cycles (SDLC) have to be not about pushing software quickly to market, but building software quickly and securely."

Five Key Insights From The Survey

The 2018 survey revealed that:

1. Web and mobile applications present the highest risk
A huge 36% viewed customer-facing web applications as the area presenting the highest security risk to businesses. Another 26% think that the biggest risk is posed by internal-facing web applications. A quarter of respondents think mobile applications are the most risky. Desktop applications and embedded and IoT systems were represented at 24% and 16% respectively. (Participants were allowed to choose multiple responses to this question.)

2. More organisations have a cyber security incident response strategy
This year, 71% of the respondents reported that they have a strategy in place in the event of a security incident, a slight improvement over last year's 66%.

3. Organisations are not managing open source risk well
Only 43% of the respondents have an established process for inventorying and managing open source software, while 30% reported that they do not. Another 27% say they do not use open source.

4. Lack of skilled security personnel is a top challenge
Fifty-six percent of those surveyed highlighted the lack of skilled security personnel or training as one of the biggest challenges to implementing an application security programme. Eighteen percent of the respondents said little or no budget is available, while 17% identified lack of management buy-in. (Participants were allowed to choose multiple responses to this question.)

5. Organisations recognise the importance of cyber security training
Eighty-three percent of those surveyed have received some form of cyber security training (mandatory or ad hoc), which underlines the importance of training to help organisations protect against threats. SST

A Pivotal Time To **Rethink** Cyber Security

►► **By Lionel Lim,** Vice President and Managing Director, Asia Pacific and Japan, Pivotal

Image: Pixabay.com


Image: Pixabay.com

The threat of a cyber security attack is something that affects every organisation and it is a problem that's only going to get costlier. According to Frost & Sullivan and Microsoft, in Asia Pacific the potential economic loss from cyber attacks can reach an astounding US$1.745 trillion, or 7% of the region's total gross domestic product. On top of financial loss, the study also found that cyber attacks lead to delayed digital transformation initiatives.

Despite several years of profuse attacks, many organisations still do not apprehend that traditional approaches are no longer effective in today's complex threat landscape. With threats evolving at a rate that makes it impossible for traditional security measures to keep up, now is the time for organisations to rethink how they approach cyber security.

Meet Cyber Security's Newest Contender: DevOps

"DevOps" is a portmanteau of "development" and "operations". This reflects the close collaborative relationship between two segments that traditionally would have been siloed from each other in the normal setup. The focus in DevOps is on reducing time to market and improving agility through rapid development and rollouts.

The relationship between DevOps and cloud computing is like wine and cheese with DevOps providing the agility and iterability required to fully unlock the cloud's features. Such a strong relationship plays an important role because the best approach to secure an organisation in today's cloud-connected world would be to create a software that's specifically designed for a cloud computing architecture.

Being agile in nature, cloud-native software is able to provide organisations a level of security that's not offered by standalone security software.

Rooted in the principles of Repair, Repave and Rotate, the following three features of DevOps will play a big role in keeping organisations safe in the ever-digitalising economy:

Built-in Security

Unlike traditional software development, where security is often an afterthought, security is integrated from the start of and throughout the entire DevOps workflow. This essentially shifts security "to the left" in a software development pipeline and enables companies to begin penetrating tests even earlier. As a result security vulnerabilities are identified and eliminated at every step of the development process and an end-to-end security element is established.

Constantly Rotating User Credentials

Humans continue to be the weakest cybersecurity link with employees regularly falling victim to phishing scams and carelessly sharing sensitive information. Equifax is a case in point. The CEO of the consumer credit reporting agency attributed the company's 2017 breach to human error. This breach saw the data of over 148 million consumers compromised and may eventually cost the company over US$600 million.

If an attacker is able to obtain a user's credentials, unauthorised access is likely to remain valid and useful for a long time. Even if an organisation is able detect this breach, the damage would have already been done by the time the breach is detected. With cloud-native software, organisations can fight against this by implementing frequently rotating credentials every few minutes or hours so that the credentials are only useful for short periods of time. Furthermore, constantly rotating credentials will render leaked credentials worthless.

An Inhospitable Environment For Malware

Unlike traditional enterprise security where steps to mitigate threats are only taken upon detection, cloud-native software takes a more proactive approach to cyber security.

Malware thrives on vulnerable software and static, unchanging systems. With cloud-native software's agile nature, organisations are constantly changing their systems and proactively combating malware threats. If required, organisations are able to patch vulnerabilities as soon as the software is available. On the other hand, it is common for enterprises to take months just to deploy patches across systems.

More Than Just A Buzzword

In the midst of their ceaseless quest to maximise flexibility and productivity for a competitive edge, organisations must also give equal priority to security. The cyber security aspect of cloud-native software for organisations, along with its business impact, is well documented. For most businesses, moving to DevOps and adopting its procedures will simply be an evolution as many already have some elements of DevOps in operation.

On the other hand, late adopters of DevOps will miss out on components that are vital to their security protocols and risk being stuck in the past chasing solutions to old vulnerabilities. SST

Security In Industrial Plants Needs A Rethink

►► **By Dr. Alexander Horch,** Vice President Research, Development & Product Management, HIMA

Images: Pixabay.com

The future of the process industry is digital, and this trend is being driven worldwide under the banners of Industry 4.0 and the Internet of Things (IoT).

Digitisation creates many opportunities for plant operators to enhance efficiency, increase flexibility and make their plants future-proof. However there is also a downside: threats to plant security arising from digitisation, especially as a result of rapidly growing and increasingly sophisticated cyber criminality.

It is clear that in this digital era, the process industry needs to switch from passive to active defense mode when it comes to cyber security in order to ensure plant security.

Be Proactive Instead Of Reactive

One case in point illustrates the grave threats that the process industry faces. In late 2017 the industrial control system (ICS) cyber security specialist Dragos announced that a safety controller (SIS) from a HIMA competitor deployed in a process facility in the Middle East had been targeted by a new malware attack and successfully hacked.

Apparently, the aim of the attacker was to disable the safety functions of the system. This plan did not succeed due to programming errors.[1] However, the safety instrumented system (SIS) was compromised and did exactly what it was supposed to: it initiated a system shutdown.

The professional execution of this attack demonstrates all too clearly how seriously plant operators need to take the issue of cyber security.

This cyber attack also represents a new dimension of cyber threats to critical infrastructure. According to current knowledge, it was specifically planned and designed to target the SIS of the manufacturer concerned. This kind of attack on an SIS is very demanding and requires significant effort. It is the fifth publicly known ICS incident to date, following Stuxnet, Havex, Blackenergy2 and Crashoverride.

Modern industrial plants are no longer autonomous but are increasingly linked to the outside world. This linkage throws up a fundamental risk of external attacks by cyber criminals. Image courtesy of HIMA Paul Hildebrandt GmbH

The importance of this attack can hardly be overestimated, because it was the first successful attack on a safety instrumented system, which is the last line of defense against a potentially catastrophic impact.

The attacker benefited from one significant set of circumstances: at the time of the cyber attack the SIS had been put in programming mode by a key switch. In an orderly configuration with the controller in run mode, where programme changes are not possible, the attackers would have faced a much more difficult challenge.

No other attacks on the same type of SIS are currently known.

The Concept Of Safety Is Changing

Although only a particular system was attacked, the incident marks a turning point for plant security.

The incident served as a wake-up call, rousing the process industry to the need to heighten its awareness of cyber security. Moving ahead the industry must focus on the interaction of safety and security.

In addition, it is clear that no SIS manufacturer can, now or in the future, promise a solution that is absolutely and always safe with regard to all eventualities and risks.

That is primarily because work processes and organisational deficiencies are still by far the most common targets for successful cyber attacks (see Figure 1). For example, system interfaces that remain open during normal operation and can be used to alter programme code give attackers a potential access point. As a consequence of this cyber attack, plant operators are now strongly advised to not rely solely on cyber secure components but instead to define an integral security concept for their own systems and consistently implement it in cooperation with manufacturers.

Safety-oriented automation solutions in industrial plants must now encompass more than just safe emergency shutdown (ESD); they must also provide effective protection against cyber attacks.

This has led to a paradigm shift. Previously, automated systems only had to be designed for safety and then simply checked periodically to verify the initially defined risk reduction.

In future, safety solutions must be regularly adjusted and extended in the interest of security. This paradigm shift affects both providers and operators of components for safety instrumented systems in equal measure.

This totally alters the perception of safety solutions. Now, a new core aspect of modern safety solutions is the ability to fend off cyber attacks in order to avoid costly shutdowns. This makes SIS an even more significant factor for plant profitability.

Standards Compliance And Level Separation As A Basis

A welcome trend is that companies in the process industry are increasingly recognising the importance of safety and security standards for the safety and economic viability of their plants. However, there are still companies that are not using fully standards-compliant SIS. That means they run a significantly higher risk of lost production and harm to people and the environment. To achieve maximum safety and security, it is especially important for plant operators to implement the requirement of the standards for functional safety and automation security (IEC 61511 and IEC 62443) for physical separation between safety instrumented systems (SIS) and process control systems (BPCS).

Standards compliance is a key aspect of defense against cyber attacks.

According to IEC 61511, safety instrumented systems and process control systems can only be regarded as independent safety levels if they are based on different platforms, development bases and philosophies. In concrete terms, this means that the system architecture must fundamentally be designed to prevent the simultaneous use of components of the process control system level and the safety level without a detailed safety analysis. Without clear separation, patches implemented in the process control system could, for example, influence functions of the integrated safety system. That can have fatal consequences.

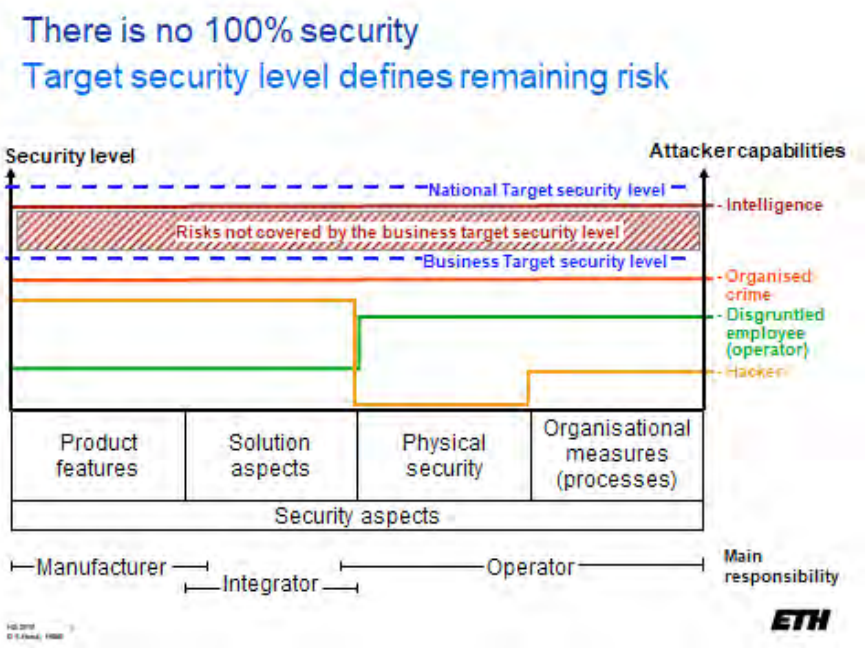


Figure 1: Complete security is an illusion. Work processes and organisational deficiencies are by far the most common targets of successful cyber attacks. Image courtesy of ETH

An equally problematic situation arises when a successful cyber attack on the process control system via the office PC of an employee results in the compromising of the integrated safety system, with the result that functional safety and basic cyber security are also compromised.

As can be seen from the above, the link between office IT and the production system always exhibits extreme weakness. An attack on an integrated SIS/BPCS system is thus considerably easier than an attack on a stand-alone SIS.

There is a lot at stake in the event of a successful cyber attack. At the worst, it can impair plant safety with incalculable consequences on the health of employees, the material assets of the company and the environment.

Cyber security insurance policies are starting to emerge. However, it is questionable whether the plant operator's insurance coverage would be fully effective in the absence of compliance with applicable standards or if blatant security deficiencies can be proven. Cyber security insurance demands clear risk assessments in

Figure 2: Both the safety standard and the cyber security standard prescribe separate protection levels. Image courtesy of HIMA Paul Hildebrandt GmbH

plants based on applicable standards. Otherwise insurance is not possible or not financially viable.

Plant operation is only reliable when plant operators systematically implement cyber security measures such as separation of protection levels in addition to functional safety.

Proactive Cyber Security Is A Must

Rapidly growing and increasingly professional cyber criminality compels both manufacturers of safety solutions and their users in the process industry to pursue proactive cyber security

policies and establish integral safety concepts. As part of risk assessment, plant operators must weigh the financial expenditures for effective safety and security concepts against the costs of potential shutdowns, which can easily run into the millions. The money invested in cyber security, usually only a fraction of the cost of a shutdown, is not wasted; it safeguards the productivity of the entire plant.

As a user, you can opt for the best possible defence by using safety instrumented systems with the fewest possible vulnerabilities.

For example, a dedicated operating system specifically developed for safety-oriented applications runs on HIMA's autonomous SIS controllers. It includes all functions of a safety PLC and omits all other unnecessary functions. There are no software components from third-party software packages and no built-in back doors. That renders typical attacks on IT systems ineffective. The operating systems of the controllers are tested for resistance to cyber attacks during the software development process. That is also ensured by security certification of the development process and by the development processes necessary for functional safety, such as the two-person principle.

However, for plant operators it is not enough to rely on standards-compliant hardware and software. Cyber security must be developed jointly by plant operators and safety specialists in the conceptual design of new plants or prior to update measures. The minimum requirement for existing plants is an exact analysis of potential cyber security weaknesses. Along with technical measures, users must also implement organisational measures, because no existing technology can provide complete protection against new forms of attack.

Consequently, there is a strong need for periodic checking of internal networks and communications systems, for example through penetration tests carried out by independent parties.

In other industries it is now common practice to allocate fixed budget amounts for recurrent safety and security audits. In these audits, external specialists conduct threat tests to thoroughly examine internal cyber security measures, with the objective of identifying and eliminating weaknesses. This basically translates to proactively employing hackers to find potential vulnerabilities that could be exploited by other hackers.

The results of these tests should be used to boost safety measures in the entire industry to a uniform and effective level. Associations and the German Federal Office for Information Security (BSI) can assist in this. The latter has already published helpful documents on the subject of cyber security in industrial control systems from the perspective of manufacturers and plant operators.[2]

Good Safety Technology Is Not Enough

The human factor is the most frequent source of cyber risks. That includes not only targeted cyber attacks aimed at disrupting production processes or stealing industrial secrets, but also disruptions that can arise from inattention. For safety-oriented systems, the usual cyber security rules are even more important because the SIS represents the last line of defense against a potential catastrophe. Protection against human penetration, whether intentional or unintentional, is therefore especially important. Consequently, a comprehensive security concept includes aspects such as specific access protection, physical safeguarding or checking the plausibility of changes. Here technology can and must form the basis for taking the pressure off people. It is also important to constantly be aware of possible means of manipulation and take them into account. In this regard, safety-critical applications are fundamentally different from other industrial PLC or office applications. Considerable expertise is necessary to ensure security in safety applications.

This is a major challenge, especially for relatively small enterprises. Maintaining and constantly refining security often poses a nearly insurmountable hurdle for plant operators. It is advisable to draw on the services of experienced safety and security experts in order to jointly develop and implement effective concepts.

Currently one of the major threats is "spear phishing" – the targeted spying out of access data for protected systems. Once employee passwords become known, launching a cyber attack is child's play. Plant operators should engage all employees and encourage them to become familiar with the issue of IT security and be part of an effective proactive cyber security strategy.

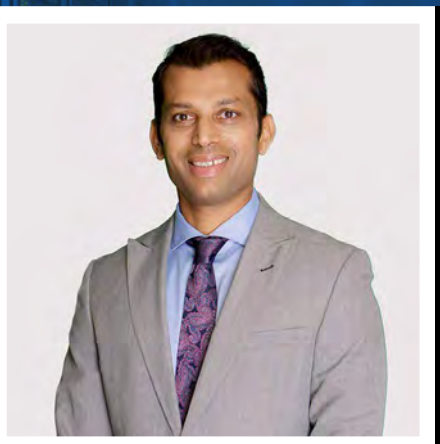
Loss or damage that arises from the action of an employee should be considered a system issue. Such loss or damage should demonstrate the necessity to fill knowledge gaps and familiarise employees with threat scenarios, such as known social engineering strategies. Security training and increasing employee awareness are thus an essential component of a proactive safety concept. SST

---

[1] *Dragos, TRISIS Malware – Analysis of Safety System Targeted Malware, version 1.20171213, link: https://www.dragos.com/blog/trisis/; and Cyberwire podcast "TRISIS Malware: Fail-safe fail – Research Saturday", link: https://thecyberwire.com/podcasts/cw-podcasts-rs-2018-01-06.html*

[2] *https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/Empfehlungen/ICS/empfehlungen_node.html*

Make 2019 A More Digitally Secure Year For Your Organisation



►► **By Sanjay K. Deshmukh,**
Vice President and Managing Director, Southeast Asia and Korea, VMware

In 2019, businesses will make a bigger push to accelerate the deployment of next-generation technologies such as blockchain, cloud and artificial intelligence in their bid to innovate and keep up with consumers' shifting preferences for digital platforms.

However, this new digital reality exposes businesses to more cyber security risks. And existing infrastructure is currently insufficient in safeguarding data, applications and users.

Poor consumer cyber hygiene amplifies this threat. The VMware Banking Consumer 2020 Study reveals that less than a third of Southeast Asia consumers (24%) practice good cyber hygiene. An earlier survey, the 2017 VMware Digital Workspace Study, reports that more than a third of workers in Southeast Asia are using unapproved personal devices for work, increasing companies' vulnerability to data breaches.

It is becoming very clear by now that today's reactive approach to enterprise security is no longer adequate to combat poor cyber hygiene practices and increased susceptibility to multiple attack vectors.

Organisations have to realise that security needs must be intrinsically built into all apps, all cloud and all devices. Furthermore, organisations need to leverage on their "home court" advantage; that is, adopt a new security model that focuses on identifying which behaviours are normal or odd within their digital ecosystem rather than trying to mitigate every single threat activity, many of which will turn out to be false alarms.

> ***"The first is to limit the attack surface. With threats coming in through countless attack vectors, perimeter-centric security will no longer work in today's cloud era."***

To ensure their businesses are secured and to achieve home court advantage in 2019, it is imperative that organisations make two strategic shifts.

The first is to limit the attack surface. With threats coming in through countless attack vectors, perimeter-centric security will no longer work in today's cloud era.

Secondly, businesses need to focus on securing data and apps to reduce security blind spots, instead of only securing data centres since data now resides in a wide range of devices.

To this end, businesses need a digital foundation built with a Virtual Cloud Network architecture, which enables organisations to respond to new opportunities and threats, create new business models and deliver services to all applications and data, wherever they are located. SST

AKAMAI'S CREDENTIAL STUFFING REPORT REVEALS A WORLD UNDER CONSTANT SIEGE

Over 8.3 billion malicious login attempts from bots in May and June 2018. That is the eye-popping revelation from Akamai's 2018 State of the Internet/Security Credential Stuffing Attacks report.

According to the American content delivery network and cloud service provider, worldwide malicious login attempts are on the rise. Akamai detected approximately 3.2 billion malicious logins per month from botnets from January through April 2018. But in May and June 2018, this figure has increased to 8.3 million a month – a monthly average increase of 30%.

From November 2017 to June 2018, over 30 billion malicious login attempts were recorded.

The term "botnet" covers everything from web crawlers to site scrapers, account takeover tools and DDoS tools. One type of botnet focuses on a tactic considered malicious by every business: credential stuffing.

Malicious login attempts result from credential stuffing, where hackers systematically use botnets to try to steal login information across the web. They target login pages for banks and retailers on the premise that many customers use the same login credentials for multiple services and accounts. Most of these attacks were launched from the U.S., Russia and Vietnam.

Virtually every business is impacted by credential stuffing botnets. Credential stuffing can cost organisations millions to tens of millions of dollars in fraud losses annually, according to the Ponemon Institute's The Cost of Credential Stuffing report. In 2018, these attacks resulted in 1.4 billion compromised usernames and passwords, according to the Akamai report.

Continually Evolving Attacks

Credential stuffing is part of an expanding ecosystem of attackers coming to your site every day, increasingly using methods that you can't detect without specialised tools.

"Our research shows that the people carrying out credential stuffing attacks are continuously evolving their arsenal. They vary their methodologies, from noisier, volume-based attacks, through stealth-like 'low and slow'-style attacks," said Martin McKeay, Senior Security Advocate at Akamai and Lead Author of the State of the Internet/Security report. "It's especially alarming when we see multiple attacks simultaneously affecting a single target. Without specific expertise and tools needed to defend against these blended, multi-headed campaigns, organisations can easily miss some of the most dangerous credential attacks."

Image: Pixabay.com

CREDENTIAL STUFFING ATTACKS

8.3 BILLION
Malicious Login Attempts
May-June 2018

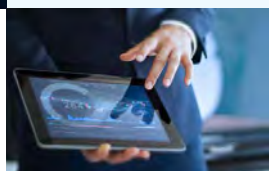
FINANCIAL SERVICES AND RETAIL
Most Vulnerable Industries

BOTNET GOALS
- Assume identity
- Gather information
- Steal money or goods

APPROACHES

LOW AND SLOW STEALTH MODE
Bots attack in rotation across many domains, hiding their activity

Large US credit union
- 10x increase in malicious login attempts in 1 week
- 3 botnets



AVALANCHE MODE
All bots attack simultaneously

Fortune 500 financial services firm
- 8.5 million login attempts in 6 days
- Most within 48 hours

WORLDWIDE CREDENTIAL STUFFING

90% OF ALL ATTACKS
Top Target Country: US

1.4 BILLION
COMPROMISED USERNAMES AND PASSWORDS IN 2018

But Attacks Can Be Contained

Akamai's Vice President of Web Security Josh Shaul shared the story of a battle against credential abuse. "One of the world's largest financial services companies was experiencing over 8,000 account takeovers per month, which led to more than $100,000 per day in direct fraud-related losses. The company turned to Akamai to put behavioural-based bot detections in front of every consumer login endpoint and immediately saw a drastic reduction in account takeovers to just one to three per month and fraud-related losses down to only $1,000 to $2,000 per day."

A Tug Of War Between Web Teams And Security Teams

One reason many organisations don't have stronger controls to prevent credential stuffing is that 70% of the people surveyed (Ponemon report, October 2017) believe the tools needed to defend against these attacks diminish the web experience of legitimate users.

The tension between web teams and security teams often revolves around user experiences, with any control that impacts the user experience, and therefore conversion rates, facing an uphill battle from the start. Clearly, credential stuffing defences need to able to function without introducing user lag to be successful.

Not My Problem

A second issue of concern highlighted by the report is that in 40% of the cases, no one function has overall responsibility for dealing with the attacks. Even in the best of organisations, lack of a clear line of responsibility often means that no one takes responsibility. At best, it means a conscientious team takes charge but faces problems because of a lack of authority. Couple this with the fact that nearly half (48%) of respondents feel their organisations lack sufficient budget to combat the issue, and it can be seen why credential stuffing defences are lagging in many organisations. Because credential stuffing is still no one's responsibility at many organisations, it will almost certainly continue to be profitable for the attacker. SST

DNS Attacks Hitting Financial Services Companies Hard

DNS THREAT REPORT REVEALS ALARMING 57% RISE IN COST OF RECOVERING FROM DNS ATTACKS IN LAST 12 MONTHS

Image: Pixabay.com

The financial services industry is the sector worst affected by DNS attacks, the kind cyber attackers increasingly use to stealthily break into bank systems, according to the 2018 Global DNS Threat Report by EfficientIP, a leading specialist in network protection.

The results are based on responses from 1,000 respondents in three regions - North America, Europe and Asia Pacific. The respondents included CISOs, CIOs, CTOs, IT managers, security managers and network managers. Financial sector organisations comprised 14% of the entire survey base.

The report also revealed that financial organisations suffered an average of seven DNS attacks last year, with 19% attacked 10 times or more in the last 12 months.

In addition, the financial cost of each attack has gone up.

Last year, a single financial sector attack cost each organisation US$588,200. This year the research shows each organisation spent $924,390 to restore services after each DNS attack, the most out of any sector. The amount translates to an increase of 57% over 2017.

Rising costs are not the only consequence of DNS attacks. DNS attacks also cost financial institutions time. The most common consequences of DNS attacks are cloud service downtime (experienced by 43% of financial organisations), a compromised website (36%), and in-house application downtime (32%).

Financial services take a very long time to mitigate an attack, requiring an average of seven hours. This recovery time is second only to the public sector. In the worst cases, some 5% of financial sector respondents spent 41 days to unscramble and recover from a DNS attack in 2017.

While 94% of financial organisations understand the critical importance of having a secure DNS network for their business, overwhelming evidence from the survey shows they need to take more action. Failure to apply security patches in a timely manner is a major issue for organisations. The report disclosed that 72% of finance companies took three days or more to install a security patch on their systems, leaving them open to attacks.

"The DNS threat landscape is continually evolving, impacting the financial sector in particular. This is because many financial organisations rely on security solutions that fail to combat specific DNS threats," commented Nick Itta, VP Sales APAC, EfficientIP on the reasons behind the attacks. SST

Recommendations

Based on its experience working with some of the world's largest global banks and stock exchanges to protect their networks, EfficientIP recommends the following five best practices:

1. Enhance threat intelligence on domain reputation with data feeds that provide menace insight from global traffic analysis. This will protect users from both internal and external attacks by blocking malware activity and mitigating data exfiltration attempts.

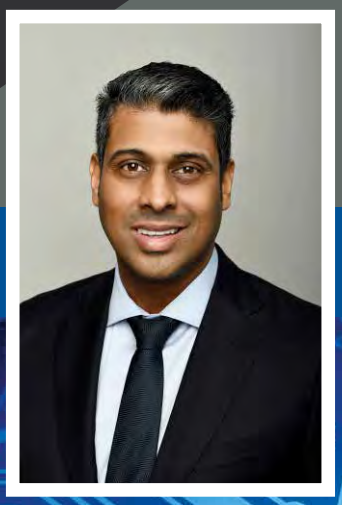
2. Augment threat visibility using real-time, context-aware DNS transaction analytics for behavioural threat detection. With this, businesses will be able to detect all threat types and prevent data theft to help meet regulatory compliance such as GDPR and US CLOUD Act.

3. Apply adaptive countermeasures relevant to threats. With this, business continuity is ensured even when the attack source is unidentifiable. It also eliminates the risk of blocking legitimate users.

4. Harden security for cloud/next-generation data centres with a purpose-built DNS security solution, which will overcome the limitations of solutions from cloud providers. This ensures continued access to cloud services and apps, and protects against exfiltration of cloud-stored data.

5. Incorporate DNS into a global network security solution to recognise unusual or malicious activity and inform the broader security ecosystem. This allows the holistic network security to address growing network risks and protect against the lateral movement of threats.

Test Drive Your Security Approach

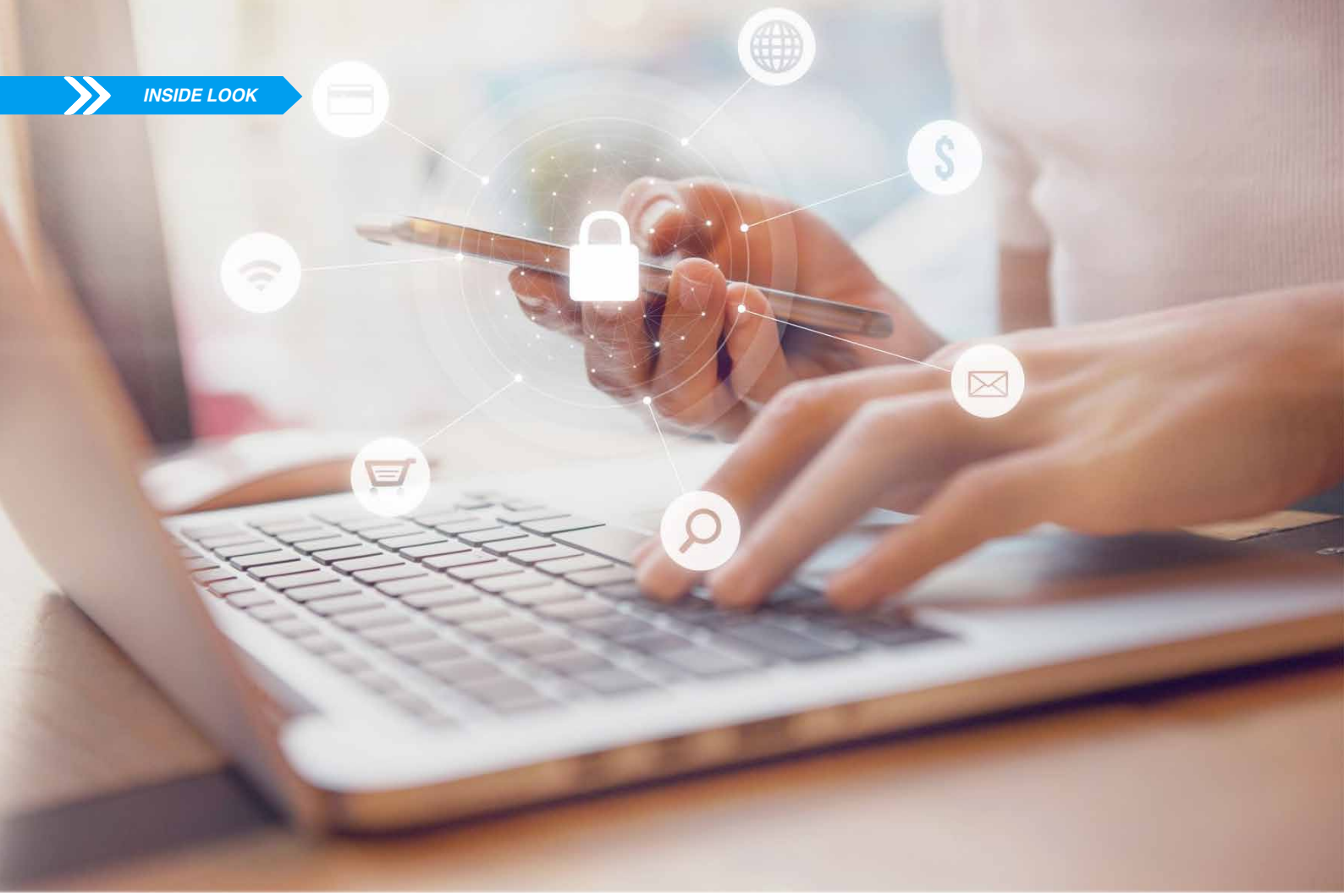


▸▸ **By Nilesh Mistry,** VP, Head of APAC, World Wide Technology (WWT)

Selecting and testing the right security solution for your organisation is a major decision. It is also time consuming. A slipshod decision here can result in downtime, data loss or worse, a network breach. Informed decisions, on the other hand, require a thorough analysis of all available offerings, which can be challenging.

A common refrain from many organisations is that they simply do not have enough time, staff, expertise or the needed infrastructure to test and select the right cyber security solution.

Just like buying a car, cyber security solutions need to be driven over several rounds on the circuit before organisations can find the most suitable and optimal solution for their needs. The best way to do this is to work with cyber security vendors to test out these solutions in a sandbox environment before actual implementation.



Always Best To Test Drive

How can organisations test and evaluate different security solutions while keeping their normal business operations running?

Organisations should select a vendor that can simulate the organisation's actual systems within a lab environment. This allows organisations to run tests on multiple solutions concurrently without affecting their day-to-day operations. This will bring about greater time and cost savings while allowing for more accurate comparison between the different solutions since they will be tested in a controlled environment.

Another advantage to this is that vendors can help organisations perform proof of concept (POC) evaluations on certain theoretical solutions in a virtual environment.

Security Training

In a fast-changing cyber security landscape, organisations need to ensure their teams are kept updated on the latest cyber security trends and cyber threats on the horizon. This is often done through frequent cyber security training. However, the exercise is often seen as boring and time-consuming owing to its staid nature.

It is possible to change boredom to engagement by creating virtual war zones in a lab and pitting customer organisations against each other. These cyber war games can be made to simulate a security environment under attack. Not only will trainees be able to apply the concepts they've learnt in a simulation, but this will certainly make the exercise far more engaging. It will also make for a good team-building activity.

Integrating Automated Solutions

Since it is difficult for many organisations to deploy a 24x7 cyber security workforce, some of them are relying on automation to respond to cyber threats. In order to do so, several OEM solutions are available on the market, though some of them may not work well together or comply with the incident response processes of the organisations.

A cyber security vendor or system integrator will be able to resolve this and ensure that organisations achieve a succinct level of automation that not only works but works seamlessly.

Partnering With Innovation Ecosystem Providers

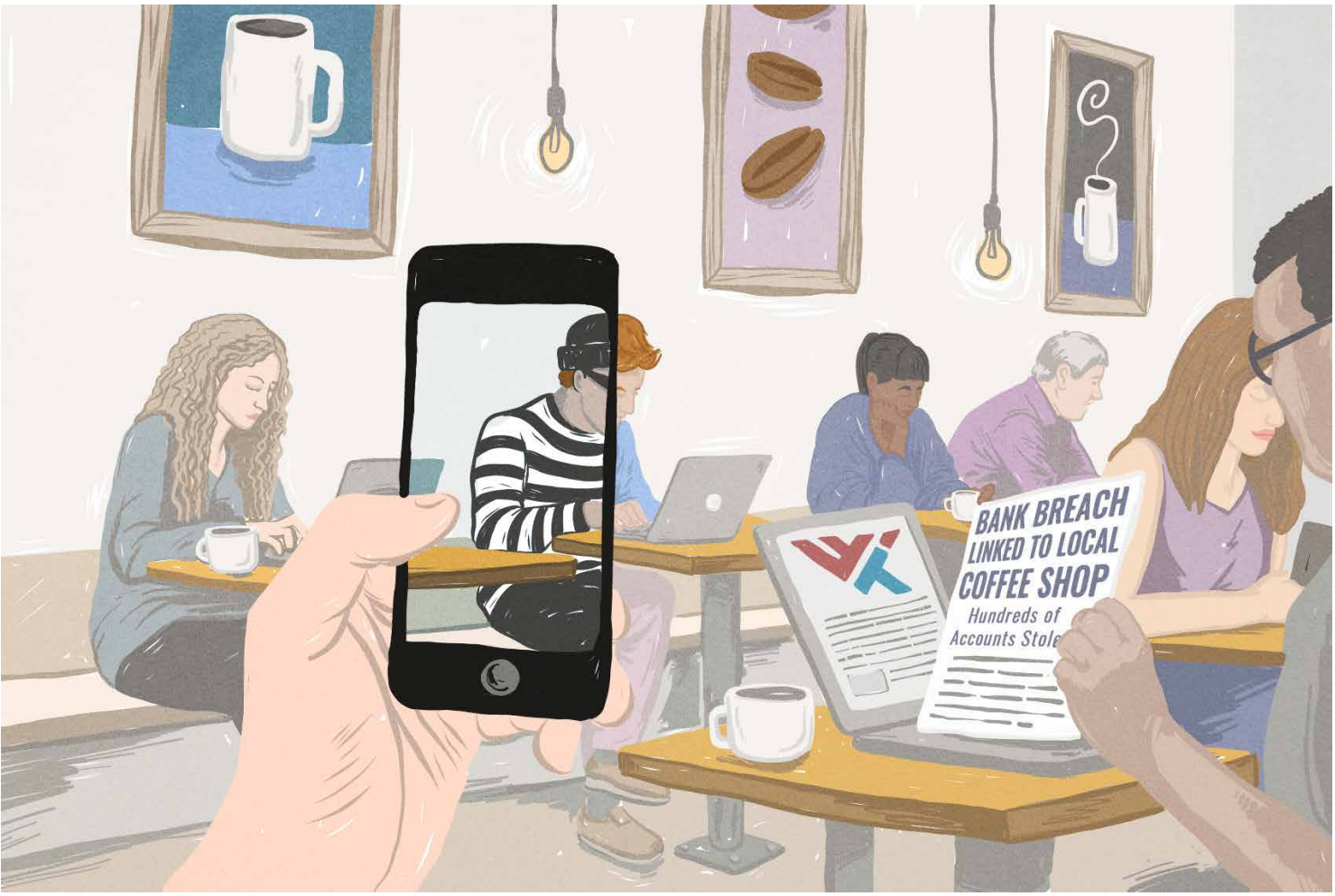
New and innovative ways to further reinforce cyber security systems are needed to address ever-

> ***"Organisations should select a vendor that can simulate the organisation's actual systems within a lab environment. This allows organisations to run tests on multiple solutions concurrently without affecting their day-to-day operations."***

changing and increasingly sophisticated cyber threats. Organisations need to constantly evaluate threats and employ emerging technologies to counteract and protect their systems from potential attacks.

Today one of the most effective ways to eliminate the pain of evaluating new technology and to achieve desired business outcomes is to work with technology partners that can offer the talent and the innovation ecosystem to test solutions. The right partners will help bring hundreds of technology companies into one environment for testing and pair their best minds with those of their customers for guidance and expertise along the way.

With threats that are evolving at lightning speed, a proactive security posture is now more critical than ever. Governments and businesses the world over now recognised that this isn't a threat that can be put on the backburner until an incident occurs. Prioritising investment in cyber security innovation is the need of the hour as organisations look to effectively manage risks in a digital world. SST



IS THE JURY STILL OUT ON BLOCKCHAIN?

Images: Pixabay.com

►► **By Tony Jarvis,** Chief Strategist - APAC, Middle East & Africa, Check Point Software Technologies

The traditional business models still in use today suffer from a number of issues. For example, the decision making function occupies a large amount of time, which ultimately impacts on project deadlines. Additionally, since most organisations consist of several tiers, messages are susceptible to being misinterpreted as they get passed on along the hierarchy.

It is processes such as these where blockchain stands to make a significant impact, with initiatives aimed at increasing both efficiency and productivity.

While owners of cryptocurrency may currently be in the minority, more than half of those surveyed indicated that they would buy these currencies in the future*. They also believed that payment via cryptocurrency would become widely accepted in the retail industry by 2025.

This is an exciting time as the market matures, moving from early adopters to mainstream awareness.

The process of making a payment via cryptocurrencies is quite straightforward. First, a wallet needs to be downloaded, which is simply an app that lets you receive, hold or spend money. Currency then needs to be moved into the wallet, with payments being made via the app. There is no need for a printed receipt as a transaction ID is issued instead, which serves as a unique fingerprint of the transaction. This can be searched on the specific cryptocurrency's blockchain where the details of the transaction are listed.

But will this trust architecture work? The answer is that we are seeing the foundations being laid right now. Various countries have anti-money laundering policies or counter financing of terrorism policies in place that specifically address cryptocurrencies. More cryptocurrency exchangers are entering the market. Ultimately, as long as the infrastructure, regulation and consumer demand exists, it will eventually become mainstream.

While the dark web has undeniably contributed to the success of cryptocurrencies, the association between virtual currencies and criminal activities is waning. Any form of money that allows for either privacy or anonymity will be lucrative for illicit activities, yet there is no shortage of real-world examples where the technology is being used in practical ways.

Cloud storage, for example, currently sees users uploading files in their entirety to a hosting platform operated by a single vendor. Using blockchain, individual files can be shredded, encrypted and distributed across multiple environments.

Blockchain has even been used to tackle the problem of counterfeit goods in Chinese markets. Imitation copies of fine wines are often sold to unsuspecting buyers. The solution? The wine importer labels each bottle with a QR code, NFC or RFID tag, each containing a cryptographic ID that cannot be duplicated. Each retailer handling the goods is registered on the blockchain, allowing wine buyers to verify the bottle's authenticity by scanning the QR code or tag.

The Security Issue With Blockchain

As with all new technologies, security is a key issue that is hotly debated. While the security of the blockchain itself isn't so much of a concern, it's often the third-party online exchanges that tend to be targeted. Most cryptocurrency users rely on these exchanges to hold their money and a number of exchanges have witnessed successful attacks in the past. The Youbit cryptocurrency exchange in South Korea suffered two attacks in 2017, which ultimately led to it shutting down and filing for bankruptcy.

One implication of the way transactions are distributed across ledgers is that it is difficult to handle situations where errors are made. Much like generally accepted accounting principles, a second transaction needs to be created to reverse the first in such cases. This is one of the challenges facing banks as they turn towards blockchain as a way of increasing efficiencies while reducing costs. One thing remains clear – there are just as many opportunities as there are challenges, and we will only see more developments centred around blockchain in due time. SST

CASE STUDY

Dahua's Surveillance Solution Keeps Train Users Safe In Brazil

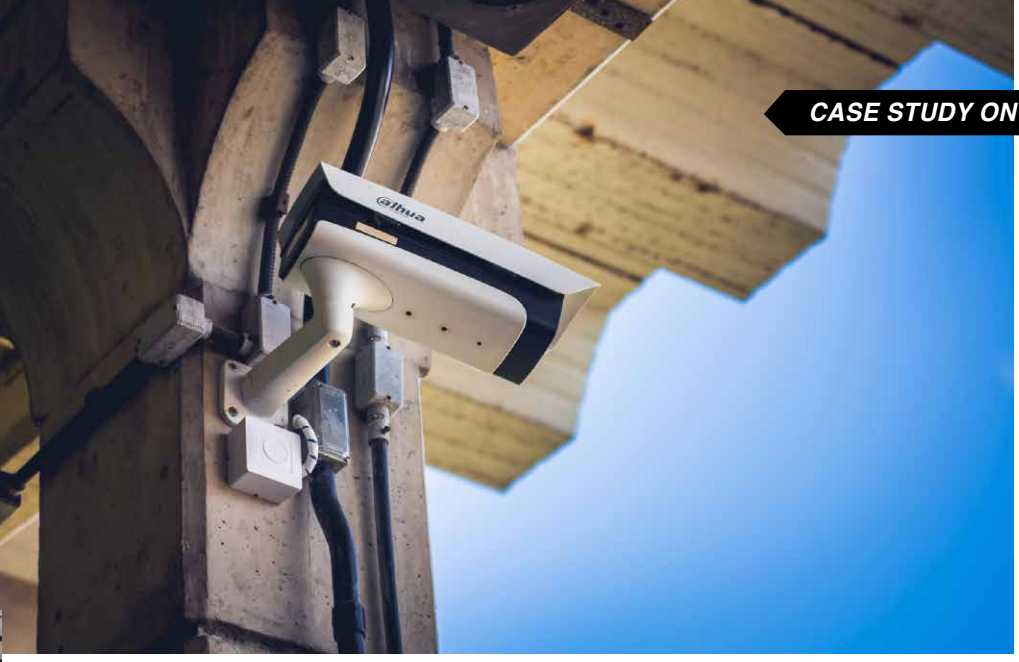
Recife's subway trains are busy, busy, busy.

The capital of the northeastern state of Pernambuco, Recife ranks third in Brazil in number of subway users. Each day, the urban train system moves 400,000 train passengers.

With this high volume of traffic, it was deemed imperative to lift security along the subway system. And so in 2017, Companhia Brasileira de Trens Urbanos (Brazilian Urban Trains Company, CBTU) embarked on a project to improve surveillance of the stations, trains, electrical systems and permanent pathways within the Pernambuco subway. A budget of BRL 61.5 million was allocated for the project.

The Solution

The challenge for the project was the need to adapt the technology chosen to the specific conditions of the subway system including difficult lighting conditions and heavy people flow while ensuring that the technology does not interfere with train service. The chosen solution must also be easy to operate and install.



In the end, the train operator decided on an intelligent surveillance network solution that would see 1,380 high-resolution cameras from Dahua Technology monitoring 52 locations scattered all over the 71 km of the railway line.

Four models of Dahua network cameras were selected: DH-IPC-HF5231EN-Z-S2; DH-IPC-HF5231EN-S2; DH-IPC-HDBW8231E-ZS2; and DH-SD65F230FN-H.

With the huge amount of data that needs to be captured and analysed daily, the H.265 video compression pattern - a format twice as efficient as its predecessor, H.264 - is essential since it uses only 50% of the bandwidth while delivering high quality images. In addition, Dahua's proprietary Starlight technology means that sharp and colourful images are generated day and night, even under difficult lighting and extreme low-light conditions as low as 0.005 Lux.

In addition to supplying the cameras, Dahua also provided professional technical support to ensure successful installation.

Detailed Views = Safer Journeys

The main features of Dahua cameras such as H.265 compression, analytics and Starlight technology allow the train operator to obtain detailed views of subway operations, even at peak hours or during tourist events such as the Brazilian Carnival. This has lifted security along the Central and Southern lines of the Pernambuco Subway.

The biggest payoff of the new surveillance network has been the boost in passenger safety. The system prevents intrusions into vital areas of operation and other occurrences that threaten passenger safety. For instance, even when video surveillance operators are not tracking the images of a specific camera, video analytics will automatically detect movements in a restricted region and send an alert to surveillance operators.

"The results have already started to be seen. We have managed to identify and arrest suspects and have handed them over to the police. We are employing all efforts to train and hire new agents and I am sure we will achieve greater gains in the future," revealed Leonardo Villar Beltrão, Superintendent of CBTU Recife.

The police is able to search the image database of recorded video footages of the subway's facilities and use features such as zoom to capture details to help its investigations.

Other Benefits

Dahua's network cameras mean that now the comings and goings of passengers along the Central and Southern lines are scrutinised by security teams in multiple locations throughout the subway's operation. This is a departure from the previous single-management model. It allows for better management of the entire security team scattered throughout the 37 stations.

In addition, the video surveillance ensures not only the physical safety of train users, but also minimises costly disruptions caused by the common problem of vandalism. A window broken by a train user can delay the routine of thousands of passengers. With the video surveillance cameras it is not only possible to identify suspects, maintenance service can be activated in a more agile way and the impact of the incident on train service reduced.

"With this project, Dahua Technology reaffirms once again its expertise in projects for the public segment. The solution offered will enable the end client to have a fully smart video surveillance system that will provide optimal lighting in dark environments, 24-hour protection of restricted areas, occurrence alerts and deliver high performance for operators," said Fabio Lopes, Channel Sales Director of Dahua Technology Brasil. SST

Images: Freepik.com

Migrating To An IP Video Surveillance Solution

All You Need To Know

The migration from analogue video surveillance to IP systems has been gathering steam for some time now, driven by decreasing costs and rapid advances in new security technologies such as video analytics.

As William Tan, NEC Corporation's Director Of Global Face Recognition & Surveillance (Global Safety Division), puts it: "The use of video analytics in surveillance systems improves operational efficiency as it eases the workload of security officers. Analytics adds value and makes the IP camera system more intelligent. Increasingly, government agencies are adopting safer city technologies such as facial recognition as they allow the authorities to have more "eyes" on the city than before."

Migration to an IP system is only a matter of time for most organisations. IP systems offer organisations an array of expanded functions from analytics and the use of non-visual sensors like fire alarms to remote access from anywhere in the world, and give organisations the flexibility to easily expand and reconfigure their network as necessary. But what should businesses take note of when migrating their system, and how should they go about it? Benjamin Low, Vice President (Asia Pacific) of Milestone Systems, offers some answers.

►► *By Benjamin Low, Vice President (Asia Pacific) Milestone Systems*

IP systems come armed with expanded functions, from analytics to remote access, while handing organisations the flexibility to easily expand and reconfigure their network. On top of all these benefits, IP solutions also offer the lowest Total Cost of Ownership.

IP systems also make storage more flexible and less costly. HC Chang, general manager of APAC (excluding China) at Promise Technology, explains: "Analogue systems may require storage to be onsite, but if an installation has many sites, or sites that are geographically disparate, this may be difficult. IP systems allow storage to be placed in whatever site makes the most sense, making the systems easier to maintain and upgrade."

While these benefits make migrating an easy decision, organisations should carefully plan out the how of their migration from analogue to IP. The cost of migration and downtime issues can be minimised if organisations invest the time to understand their security needs and thoroughly plan the execution of the migration. The reward from meticulous planning is that companies can reap the benefits of IP surveillance faster.

Analyse Thoroughly, Design Thoughtfully

For organisations, the process should start with a full analysis of their security requirements. This involves looking at the varying levels of security needed in different areas and sites as well as the finer details of surveillance needs.

Once these requirements are uncovered, the next step is to design a detailed blueprint for the new IP system.

With the blueprint in hand, it is now time to develop a plan for deployment. Organisations looking to migrate to an IP network have two options: upgrade the whole network in one go or upgrade in stages.

Upgrading the whole system in one go simply involves removing all the old equipment and installing the new IP system. In a way this is the simpler option, as it means all the new IP features will be ready to go once installation is complete. However, installing all that equipment – not to mention the equipment itself – can be costly, especially for medium and large organisations that need to replace a great number of infrastructure and assets. Another disadvantage of this option is the inevitable downtime between the old system going offline and the new system starting up.

The cost pressure can be forbidding and downtime is unacceptable for most medium and large organisations. For these reasons, the more popular option is to upgrade in phases.

This is possible with IP surveillance systems because all cameras and sensors feed into a central VMS. The optimal VMS would be open source, meaning it is able to manage feeds from many different types of visual and non-visual sensor, both legacy and new, from many different manufacturers at the same time. This allows a surveillance network to evolve as the organisation's surveillance requirements change.

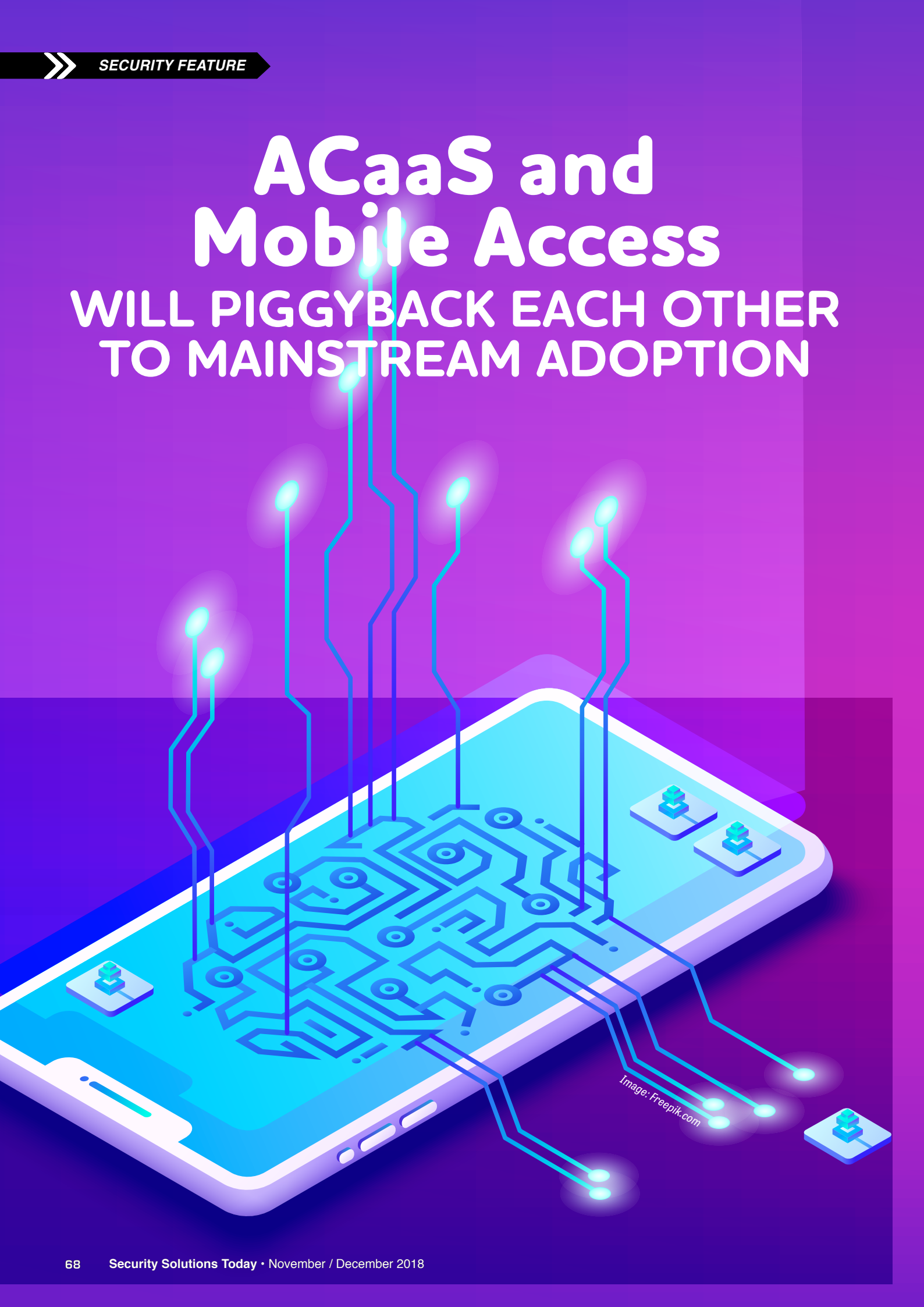
This capability is especially useful in large installations that comprise many different buildings and have varying levels of surveillance requirements throughout the installation. Some areas, for instance, may have need for higher security, requiring new high-resolution digital cameras and video analytics functions such as facial recognition.

An important point to note is that migrating to an IP system does not require the replacement of existing cable infrastructure. Winston Goh, head of marketing, South APAC, Axis Communications, notes: "Pulling out and replacing existing infrastructure, such as coaxial cables and analogue cameras, can be a very expensive process. The benefit of migrating to an IP solution is that converter devices can be used to convert the analogue signal to a digital one, so it can be fed into the VMS. This allows sections and assets to be upgraded in a way that suits the budget and requirements of each organisation. It also greatly reduces any installation downtime."

Once the deployment plan is ready, installation can begin. The undertaking kicks off with the installing of the VMS, which will be the heart of the network. You can then install new cameras and prepare old cameras to feed into the new VMS, as well as install monitoring equipment such as PC monitors at your own pace. SST

ACaaS and Mobile Access

WILL PIGGYBACK EACH OTHER TO MAINSTREAM ADOPTION



The markets for access-control-as-a-service (ACaaS) and mobile access are experiencing similar strong growth, reports IHS Markit.

It estimates revenue for the ACaaS market will increase to US$950 million by 2022. Global mobile credential downloads are forecast to increase at a compound annual growth rate (CAGR) exceeding 100% from 2017 to 2022.

HIS Markit predicts that about 20% of the current installed base of access control readers will be mobile capable by 2022. And the global information provider expects more businesses to integrate both solutions five years from now.

Said Jim Dearing, senior security and building technology analyst at IHS Markit, "While there have been relatively few attempts to combine ACaaS solutions with mobile access despite their apparent synergies, this type of integration will become more common over the next five years."

Accordingly to him, there are several compelling reasons to integrate ACaaS and mobile access.

#1 A significant segment of ACaaS end users opts for fully managed solutions. Providers of managed solutions would benefit from the ability to issue and decommission credentials remotely, allowing them to lower management costs.

#2 Both mobile access and ACaaS are typically sold via subscription, or using recurring fee-based pricing models. Adding mobile credentials to an ACaaS contract would not be an issue for an integrator, and as mobile access becomes more popular in the traditional access control market, end users and installers are likely to become more familiar with the recurring-fee pricing model, which should generate additional interest in ACaaS.

#3 Like ACaaS solutions, the majority of access control solutions are cloud based. As both become more popular, end users are likely to become more comfortable deploying cloud-based security solutions.

#4 ACaaS is increasing the penetration of access control systems in buildings, and many end users are owners of small and medium-sized businesses who have never owned an access control system before. This situation poses an excellent opportunity for mobile access, as providers can ensure that mobile-capable readers are installed from the outset.

Barriers Ahead

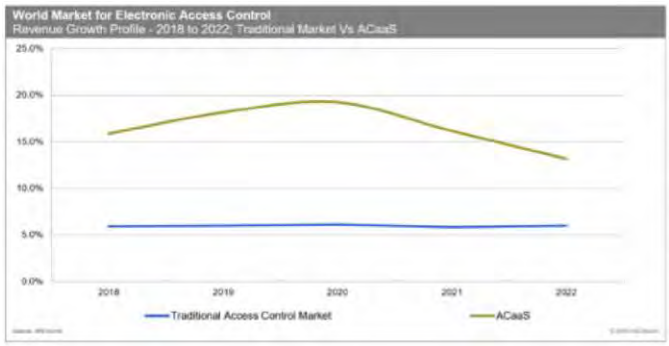
However Jim Dearing also notes that there are barriers to integrating the two solutions.

Currently, early adopters of each solution are based in different industries. Mobile access has seen its strongest adoption in the education and hospitality sectors, while ACaaS is gaining traction with small and medium-sized businesses and the property management segment.

Also due to the large number of smaller projects, a significant portion of ACaaS end users value affordability over advanced feature sets and functionality. The main adopters of ACaaS solutions are small and medium-sized businesses. They account for 21% of market revenues in 2017.

ACaaS providers may struggle to convince end users to install readers that are mobile-capable but also more expensive.

Finally, despite both solutions typically being billed on a monthly or annual basis, the pricing models vary slightly. ACaaS solutions are priced according to the number of doors, while mobile access is priced according to the number of credentials or users. Creating an intuitive but optimal pricing model for the combined solution could prove tricky for suppliers. If both original metrics are kept, suppliers are likely to encounter difficulty as end users scale their solutions. SST



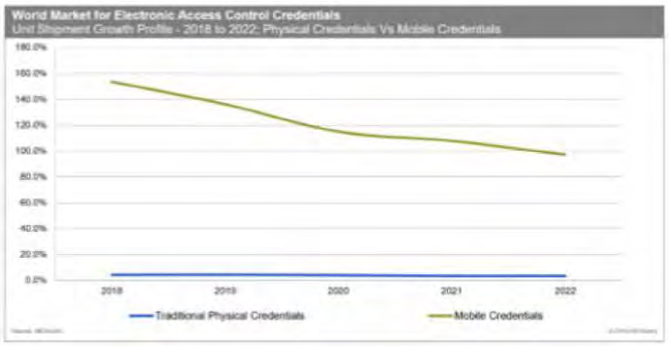


Image: Freepik.com

Predicts IHS Markit

Alexa Guard Will Make Waves In DIY Security And Insurance Domain

Blake Kozak, Principal Analyst, Smart Home and Security Technology, IHS Markit

You may be tempted to use a more expensive security system, but what if you can create a similar system using gadgets that you already have in your home?

Amazon promises just that with its recently announced Alexa Guard, a home security feature that protects homes.

It turns every Echo device – speakers, subs, link amps, buttons – into a security system by having them listen for certain sounds like the breaking of glass.

Here's how it works: When you're about to leave home, you tell Alexa you are leaving and Alexa Guard turns on. Alexa Guard will then listen for sounds that suggest burglary or the fire and carbon monoxide alarms going off.

Should Alexa Guard hear something, it alerts the homeowner via phone notification, or sends a notification to the homeowner's security provider.

Once enabled, Alexa will watch over the home while the homeowner is away.

Why Alexa Guard

It's more economical to get a similar level of protection with the gadgets that are already in your home. For the consumer DIY market, Alexa Guard is a big step forward, because there are not many options available for systems like Ring – or even SmartThings, which supports a variety of radio-frequency (RF) technologies. With Alexa Guard, consumers would save because they would not have to purchase additional hardware.

Perhaps the biggest implications of Alexa Guard will be for the insurance and fire detection market, said Blake Kozak, Principal Analyst, Smart Home and Security Technology, at information provider IHS Markit. "Larger homes require many detectors per home, so to outfit a 2,500 square foot home with Nest Protect or First Alert Safe & Sound could cost thousands of dollars. As insurance providers look to expand beyond water leak detection and security monitoring, this could have a major implication for Roost and other device makers that rely heavily on insurance providers."

In the Americas, Amazon Echo's installed base of insurance policyholders with an insurance "skill" enabled will reach about 500,000 by the end of this year, according to IHS Markit. Most of the benefits of Alexa Guard will accrue to the do-it-yourself market (DIY), rather than for professional security monitoring. Since most professional security systems already include a break-glass sensor, the effect of Amazon's announcement on the professional security industry is questionable.

Although it's possible for an audio clip to be sent to a central monitoring station, doing so would be a step backward for the professional market, which at this point should be pushing for video verification to confirm burglaries and other emergencies. Also, in the event of a home intrusion, it is unlikely the Alexa Guard feature will allow security monitoring providers to follow a burglar throughout a home, assuming multiple Echo devices are active. Instead, the central monitoring station will receive a recording of when the event happened.

For Amazon, the ability to alert users when smoke and carbon dioxide alarms go off could have a bigger payoff for possible partnership expansions with insurance companies, rather than with security providers. The fact that Amazon announced ADT as one of the partners is significant, said Blake Kozak, because Google just recently announced a partnership with Vivint to add a Google Mini with every new account.

When it comes to interactive security (such as arming and disarming security features remotely), ADT enjoyed a sizable 16-point lead over Vivint in terms of overall market share in 2017. However, Vivint enjoyed a 4-point lead over ADT in the home automation market, which includes lighting control, door lock management and other features.

It is clear Alexa Guard will have more influence on the insurance market than on professional security monitoring, declared Blake Kozak.

He predicts that Roost, Nest Protect and Kidde RemoteLync and other devices could eventually turn out to be the latest casualties of the Amazon Alexa ecosystem. SST

Image: Freepik.com

Carbon Black Introduces Powerful Threat Hunter

In this era of undetectable cyber threats, reactive defence tactics have become inadequate. In November, next-generation endpoint security provider Carbon Black responded to this challenge by launching advanced threat hunting and IR capabilities on its Cb Predictive Security Cloud (PSC).

Most endpoint detection and response and incident response tools on the market collect only a limited set of historical data. As a result, organisations struggle to get their hands on the information they need to investigate, proactively hunt and remediate.

Cb ThreatHunter solves this problem by continuously collecting unfiltered data on the PSC, a cloud-based endpoint security platform with a single agent and single console to consolidate prevention, detection, response, managed services and advanced threat hunting.

This gives security teams all the information they need to proactively hunt threats, uncover suspicious behaviour, disrupt active attacks, repair damage quickly and address gaps in defences. Investigations that often take days or weeks can be completed in just minutes with Cb ThreatHunter.

"Cb ThreatHunter has simplified incident response by allowing quick discovery of both simple and advanced threats, and quickly making decisions to take conclusive actions," said Denis Xhepa, IT Systems Security Engineer at MidCap Financial. "Its simplicity and responsiveness is amazing, especially when you are running an investigation where every minute matters. When I find something, I can prevent it for the future, and also look for other related or similar things. All this can be done very intuitively. Anomaly detection is also going to be enhanced by the backend intelligence applied to the data. Endpoint security used to be difficult."

"The combination of rapidly searchable, unfiltered endpoint data for advanced threat hunting with an array of prevention and response capabilities built into one endpoint sensor is a significant step forward," commented Marc Brawner, Principal at Kroll's Cyber Risk Practice. "Cb ThreatHunter further enhances our ability to deliver rapid incident detection and response to our global customers."

Cb ThreatHunter empowers security teams with three features:

- **Elastic Cloud Scalability:** Cb ThreatHunter is delivered through PSC, a platform that consolidates multiple critical endpoint security capabilities supporting both IT and security operations. This allows security teams to rapidly deploy and scale the solution across their enterprise without investing in (or maintaining) on-premise infrastructure, thus simplifying their operations and allowing them to focus on hunting and responding to threats.

- **More Powerful Search Fields:** Security teams can flexibly hunt threats, even if an endpoint is offline. The solution provides visibility at every stage of an attack with intuitive attack-chain visualisations and uncovers advanced threats while minimising attacker dwell time. This insight makes available immediate answers with comprehensive behavioural context so that security teams can stop attacks as quickly as possible.

- **Enhanced Threat Intel Matching:** The advanced detection capabilities allow security teams to proactively explore environments for abnormal activity, leverage cloud-delivered threat intelligence and automate repeat hunts. Additionally, the PSC's platform extensibility allows developers to create custom watchlists to power real-time detection and correlate data across the security stack. SST

Growth In Police Body-worn Cameras Drives Market For Digital Evidence-management Software

Image : Freepik.com


Image: pixabay.com

Across the world, policemen no longer just wield handcuffs, firearms and tasers. More and more of them are also packing a body-worn camera.

So widespread is the practice, more than 1.5 million body-worn cameras are in use worldwide today, most of them worn by law enforcement officers.

According to a report by IHS Markit, the global installed base for law enforcement and police body-worn cameras is forecast to increase by nearly 30% in 2018.

As the demand for the device increases so do the requirements for sophisticated digital evidence management ecosystems to manage, index and store the huge volumes of collected digital evidence.

Digital evidence-management software is software used to manage multimedia digital evidence. The capabilities of digital evidence-management software can range from simple media storage to sophisticated investigation and case-building tools.

At the entry level, the software manages the storage of video captured through a body-worn camera or an in-car video surveillance system. However, the initial ingest of media from the recording device does not need to be within the digital evidence-management software. The software can act as a platform to connect existing repositories and device configuration applications. Digital evidence software can be bundled with body-worn cameras or in-car systems or sold separately.

Today, with this great number of body-worn cameras in use and an associated increase in potential evidence collection, the capabilities of underlying digital evidence-management systems are becoming an increasingly critical factor in the ability of law enforcement to effectively manage and interpret huge repositories of digital evidence.

A Rapidly Evolving Market

The market for digital evidence-management software has evolved rapidly since federal funding programmes in the United States for law enforcement body-worn cameras were announced in 2014, detailed IHS Markit in its Body Worn Cameras & Digital Evidence Management Report released in September.

This funding and subsequent initiatives stimulated and accelerated increases in shipments of body-worn cameras in the United States and globally, setting off the current trajectory toward increasingly sophisticated digital evidence-management solutions.

The capability of digital evidence-management ecosystems has evolved over the years, with the evolution occurring in four distinct stages with increasing levels of feature sophistication from tier one to tier four. As the ecosystem evolves and integrates further with records management systems and other existing law enforcement workflows, law enforcement agencies are able to gain additional efficiencies and insights from digital multimedia evidence. SST

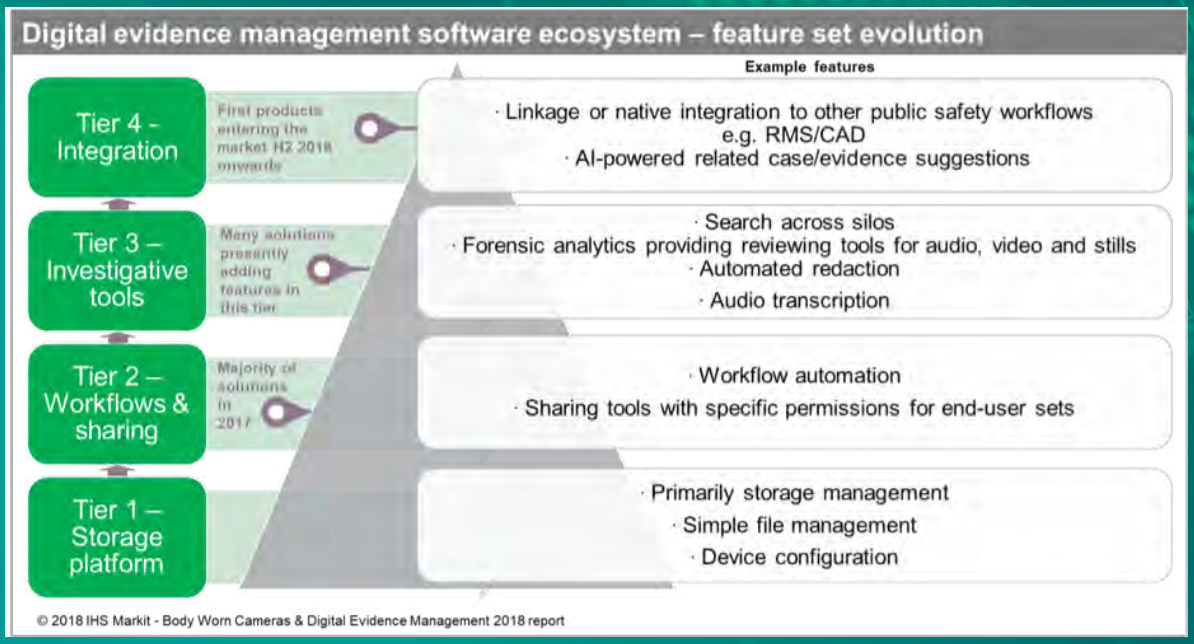


Image: Freepik.com

Secure Bank

Blocking Bank Fraud And Cyber Attacks Early

No sector suffers as much financial fallout from cyber crime as banks.

In 2017, financial services bore the highest annualised cost of cyber crime at US$18.28 million. When a bank suffers a cyber security incident involving its online banking services accounts, it costs that bank an average of US$1.75 million to resolve the incident, according to a 2017 Kaspersky Lab report.

There is no let-up ahead either; banks will likely continue to be a primary target for cyber criminals. Which means banking institutions must augment current efforts on detecting blended attacks that combine phishing, malware and fraud across multiple channels.

Which is why banks may be interested in Secure Bank, a new product launched by Group-IB that promises to prevent client-side bank fraud and attacks across sessions, platforms, devices, channels and entities.

Group-IB specialises in the prevention and investigation of cyber crime. It is the first Russian supplier of threat intelligence solutions to be recognised by Gartner, Forrester, and IDC and it has the largest laboratory of computer forensics in Eastern Europe.

Group-IB's extensive expertise in computer forensics, threat intelligence and detection allows it to build up a broad spectrum of data: "smart" behaviour analytics, anomaly detection data, daily updates of rules and signatures, as well as 100,000+ threat actor profiles. This allows it to alert banks to new attacks and fraud schemes unknown to any other anti-fraud systems.

Secure Bank leverages Group-IB's experience in threat intelligence, signature, behavioural and cross-channel analytics to detect threats invisible to traditional transactional anti-fraud systems. It is equipped with anti-fraud technologies that protect banks and bank customers across all layers while identifying fraud at the preparation stage. It can block thefts in real time and detect attacker's logins, social engineering scams, botnets, money laundering, and the possible infection or compromise of a user's device.

Smarter Data. Smarter Analysis.

Secure Bank continuously processes 9.5 million sessions a day where it compares and analyses the behaviour of both real users and those of fraudsters. By using a number of bio-chronometrics parameters (such velocity and navigation, mouse movements, keystrokes, typing cadence and delays.), Secure Bank can apply behavioural analytics to identify if a legitimate user or fraudster is logged in, reducing false positives by 79%.

Preventing Cross-banking Fraud And End User Attack

The number of thefts involving Android Trojans has increased constantly and continued to grow in 2018. Secure Bank extends the range of analysed channels to mobile devices in order to protect bank payments on smartphones, tablets and other iOS and Android devices. The Secure Bank module can either be loaded alongside bank pages on the end client's device or as an SDK in mobile banking applications.

Secure Bank also works to block cross-banking fraud. With recent regulatory initiatives such as Payment Service Directive (PSD2), which creates new points of interaction between banks and fintech services, cross-channel analysis and entity linking have become crucial for financial institutions. Secure Bank's unique adaptive logic makes it possible to correlate users' behaviour on their devices as they interact with their bank through various channels, as well as their behaviour across different banks to prevent cross-banking fraud. Machine learning algorithms and advanced rule engines allow the system to detect unusual or suspicious activity initiated by a criminal impersonating a real user.

While traditional anti-fraud systems analyse transactions, they do not have the ability to detect possible malware infections on the user's device nor any suspicious activities that could have taken place on the device before the transactions occurred. Secure Bank is able to do this, according to Group-IB.

"Secure Bank enables a bank to ensure the highest standards of customer protection possible by detecting fraud before it actually takes place. It significantly enhances the security of banking transactions, both for individuals and for legal entities," says Pavel Krylov, Head of Secure Bank/Secure Portal.

"We have created a "smart" product that incorporates unique Group-IB technologies including an extra system of identification for customer devices (device fingerprinting), a number of patented methods of detecting remote connections and in-house methods of machine learning."

Secure Bank is already trusted by Russia's leading banks and e-commerce portals. It is used to protect tens of millions of users, both private individuals and legal entities, of Sberbank Online and Sberbank Business Online. Secure Bank has also been tested by several European banks. SST

Big Data & AI Asia 2018
4 - 5 December 2018
Suntec Singapore Convention & Exhibition Centre, Singapore

2,000 To Attend 2nd Big Data & AI Asia

Corp's Big Data & AI Asia Conference And Exhibition is back on 4th and 5th of December for its second edition at Suntec Singapore. This edition is supported by over 40 sponsors and will feature more than 30 Tech Talks offering solutions to technological challenges.

Big Data & AI Asia 2018 promises to reveal critical know-hows and data acquisition trends as well as offer tips on the monetising of real-time data, machine learning and the practical use of AI.

It is expected to draw 2,000 data and AI professionals and business leaders from organisations like A*STAR, Accenture, AI Singapore, Akamai, the Defence Science and Technology Agency of Singapore, Grab, the Singapore Armed Forces and Vodafone. Sectors represented include banking and finance, insurance and investment, telecoms, media, retail and manufacturing, e-commerce and healthcare.

Attendees will receive first-hand information from big data and AI experts from global organisations that will help their enterprise make effective use and management of their data and AI development. The event also presents the opportunity for enterprises to network and forge new relationships and benchmark themselves against businesses that have succeeded in the big data and AI space. SST

Subscription Form

Fax your order today
+65 6842 2581

(Please tick in the boxes)

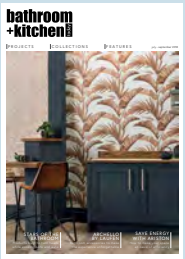
Southeast Asia Building

SINCE 1974

☐ 1 year (6 issues)

Singapore	S$45.00
Malaysia / Brunei	S$90.00
Asia	S$140.00
America, Europe	S$170.00
Japan, Australia, New Zealand	S$170.00
Middle East	S$170.00

Bathroom + Kitchen Today



SINCE 2001

☐ 1 year (4 issues)

Singapore	S$32.00
Malaysia / Brunei	S$65.00
Asia	S$80.00
America, Europe	S$130.00
Japan, Australia, New Zealand	S$130.00
Middle East	S$130.00

Southeast Asia Construction

SINCE 1994

☐ 1 year (6 issues)

Singapore	S$45.00
Malaysia / Brunei	S$90.00
Asia	S$140.00
America, Europe	S$170.00
Japan, Australia, New Zealand	S$170.00
Middle East	S$170.00

Lighting Today

SINCE 2002

☐ 1 year (4 issues)

Singapore	S$32.00
Malaysia / Brunei	S$65.00
Asia	S$80.00
America, Europe	S$130.00
Japan, Australia, New Zealand	S$130.00
Middle East	S$130.00

Security Solutions Today

SINCE 1992

☐ 1 year (6 issues)

Singapore	S$45.00
Malaysia / Brunei	S$90.00
Asia	S$140.00
America, Europe	S$170.00
Japan, Australia, New Zealand	S$170.00
Middle East	S$170.00

IMPORTANT

Please commence my subscription in _____ (month/year)

Personal Particulars

NAME: _____

POSITION: _____

COMPANY: _____

ADDRESS: _____

_____

TEL: _____ FAX: _____

E-MAIL: _____

Professionals (choose one):

☐ Architect ☐ Landscape Architect ☐ Interior Designer ☐ Developer/Owner

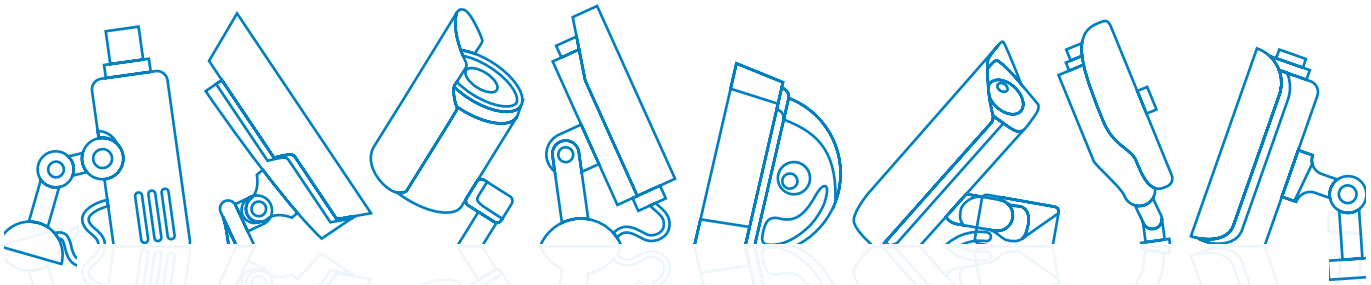
☐ Property Manager ☐ Manufacturer/Supplier ☐ Engineer ☐ Others

☐ I am sending a cheque/bank draft payable to:
Trade Link Media Pte Ltd, 101 Lorong 23, Geylang, #06-04, Prosper House, Singapore 388399
RCB Registration no: 199204277K * GST inclusive (GST Reg. No: M2-0108708-2)

☐ Please charge my credit card (circle one): Amex / Diner's Club

Card Number: _____ Expiry Date: _____

Name of Card Holder: _____ Signature: _____



Security Solutions Today

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

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

Scan to visit our website

WE ALSO PUBLISH

bathroom + kitchen today

SEAB SOUTHEAST ASIA BUILDING

SOUTHEAST ASIA CONSTRUCTION

lighting today

CREATOR OF

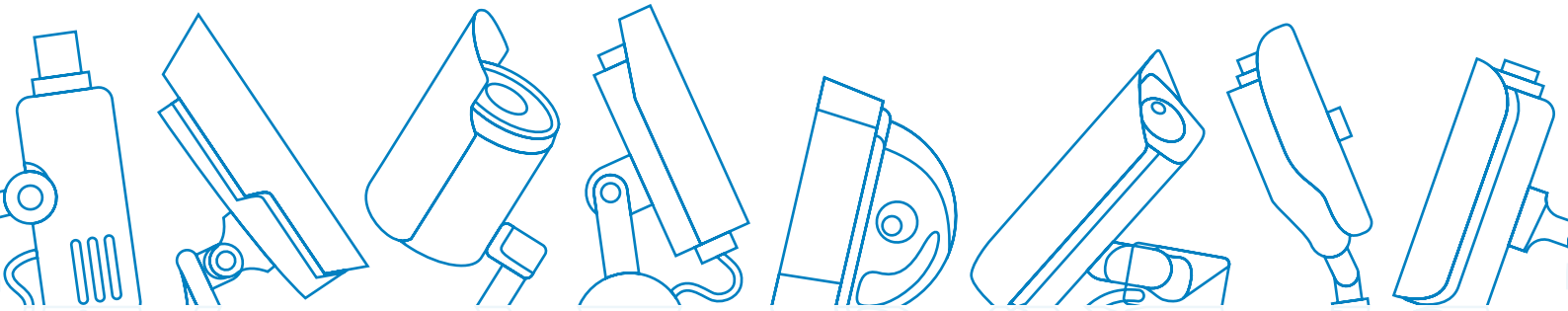
TRADECARDS GLOBAL

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

ADVERTISERS' INDEX

Our tribute to Safety & Security...



TradeCards Global mobile application is offering **50% discount** for one-year organisation listing to suppliers and service providers that serve our Safety & Security Community. With the reduced price of USD500 / *SGD700 for one-year organisation listing, suppliers and service providers get to enjoy an ***additional 10MB of product listing*** tagged to your organisation listing.

Visit **www.tradecardsglobal.com** to sign up for a new account and your organisation listing. Input "**SECURETRIBUTE**" as promo code before proceeding to payment page. The promo code is valid until 31 December 2018.

*Rate excludes 7% GST applicable for Singapore-registered companies

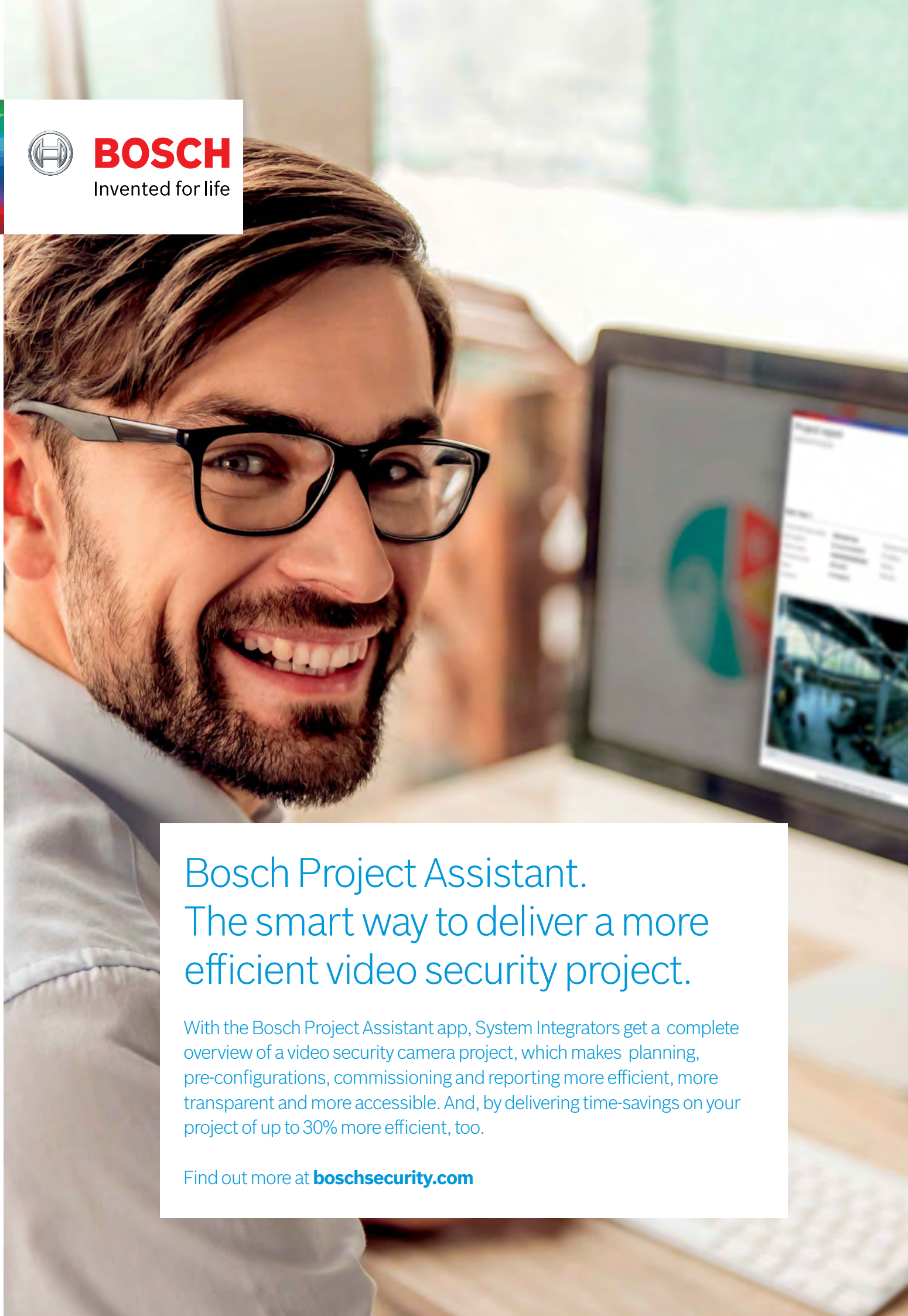
TRADECARDS GLOBAL

Supporting mobile version of:

SEAB · SOUTHEAST ASIA CONSTRUCTION · Security Solutions Today · bathroom + kitchen today · lighting today

GET IT ON Google Play

Download on the App Store



BOSCH
Invented for life

Bosch Project Assistant. The smart way to deliver a more efficient video security project.

With the Bosch Project Assistant app, System Integrators get a complete overview of a video security camera project, which makes planning, pre-configurations, commissioning and reporting more efficient, more transparent and more accessible. And, by delivering time-savings on your project of up to 30% more efficient, too.

Find out more at **boschsecurity.com**