A Lynchpin Media PUBLICATION

intelligent CISO

security intelligence that transcends borders

Trusting in CISOs
Why CISOs are being recognised as the new Chief Trust Officer for their organisations

Smart solution
Is AI the way for SOCs to work smarter and lighten the load?

Zero Trust
Why this approach has become a non-negotiable for businesses

issue 47 | www.intelligentciso.com

PATIENT PROTECTION

Daniel Maier-Johnson, CISO at Asklepios, explains how one of Germany's leading hospital operators is ideally placed to meet the needs of today and tomorrow whilst bolstering its reputation as a trusted, security-conscious healthcare group.

SECURITY PREDICTIONS 2022 REPORT

14 CYBER SECURITY PREDICTIONS FOR 2022 AND BEYOND

The Mandiant Security Predictions 2022 report examines the impact of technology, workplace trends, changes to legislation and attacker behaviors to foreshadow major cyber issues.

Experience or download the report:
experience.mandiant.com/security-predictions-2022/p/1

MANDIANT®

intelligent CISO
security intelligence that transcends borders

contents

intelligent CISO
security intelligence that transcends borders

issue 47

48. feature

The shift to remote working has highlighted a need for organisations to adapt to an identity-centric approach to their cybersecurity and governance strategies. **Craig Ramsay, Senior Solution Consultant, Omada**, discusses the management of identities and their associated risk and how business leaders can strengthen their security strategies for the year ahead.

Lynchpin Media

LYNCHPIN MEDIA TEAM

MANAGEMENT

Managing Partner: **Richard Judd**, richard@lynchpinmedia.com (+44 7534 132 966)

Managing Partner: **Stuart Lynch**, stuart@lynchpinmedia.com (+44 7514 807 117)

MAGAZINE CONTACT

Managing Editor, *Intelligent CIO Europe*, *Intelligent CISO* and *Intelligent Data Centres*: **Alix Pressley**, alix@lynchpinmedia.com (+44 20 3026 6825, Ext 1003)

EDITORIAL

Editorial Director: **Mark Bowen**, mark@lynchpinmedia.com (+44 20 3026 6825, Ext 1004)

Managing Editor, *Intelligent CIO Middle East*, *Intelligent CIO Africa* and *Intelligent Tech Channels*: **Manda Banda**, manda@lynchpinmedia.com (+44 20 3026 6825, Ext 1009)

Managing Editor, *Intelligent CXO*, *Intelligent SME.tech*: **Rebecca Miles**, rebecca@lynchpinmedia.com (+44 20 3026 6825, Ext 1007)

Senior Editor, *Intelligent CIO LatAm* and *Intelligent Tech Channels LatAm*: **John Rodríguez**, john@lynchpinmedia.com

Editor, *Intelligent CIO LatAm* and *Intelligent Tech Channels LatAm*: **Natália Moraes**, natalia@lynchpinmedia.com (+55 61 99202-7509)

Editorial Coordinator: **Louise Mair**, louise@lynchpinmedia.com

Assistant Editor: **Catherine Darwen**, catherine@lynchpinmedia.com

Editorial Assistant LATAM: **Jéssica Castro**, jessicadicastro@lynchpinmedia.com

WEB SERVICES/DESIGN

Director, Design and Production: **Pippa Sanderson**, pippa@lynchpinmedia.com

Director, Digital Services: **Charles Brandreth**, charles@lynchpinmedia.com

Manager, Graphic and Digital Design: **Daniel James**, daniel@lynchpinmedia.com

Web Designer: **Ben Fillery**, ben@lynchpinmedia.com

Graphic Designer: **Lee Jeffree**, lee@lynchpinmedia.com

Marketing Coordinator: **Harry Rogers**, harry@lynchpinmedia.com

COMMERCIAL

Director, Strategic Content: **Jess Abell**, jess@lynchpinmedia.com (+44 20 3026 6825, Ext 1005)

Director, Agency Partnerships: **James Hardy**, james@lynchpinmedia.com (+44 20 3026 6825, Ext 1012)

Director, Global Sales: **Carmen Aston**, carmen@lynchpinmedia.com (+44 20 3026 6825, Ext 1010)

Regional Director, Middle East: **Rob Chandler**, rob@lynchpinmedia.com (+971 50 8172788)

Head of Sales, UK/I and APAC: **Brett Youngman**, brett@lynchpinmedia.com (+44 7377 736116)

Head of Sales, Central Europe: **Michal Zylinski**, michal@lynchpinmedia.com (+44 20 3026 6825, Ext 1002)

Head of Sales, LATAM and Southern Europe: **Alicia Rebagliato**, alicia@lynchpinmedia.com (+34655041325/+44 20 3026 6825, Ext 1014)

CLIENT SERVICES

Head of Campaign Delivery: **Curtis Driscoll**, curtis@lynchpinmedia.com (+44 20 3026 6825, Ext 1008)

Head of Client Services: **Tom Bush**, tom@lynchpinmedia.com (+44 20 3026 6825, Ext 1011)

Accounts and Administration Manager: **Megan Kibble**, meg@lynchpinmedia.com

Campaign Executive: **Alice Tatlow**, alice@lynchpinmedia.com

Client Services Executive: **Holly Jones**, holly@lynchpinmedia.com

Operations and Client Services Assistant: **Dominic Williams**, dominic@lynchpinmedia.com

Intelligent CISO is a Lynchpin Media publication for IT security professionals with an interest in global events. If you wish to subscribe for regular copies, then please email: info@lynchpinmedia.com

Lynchpin Media is a boutique publisher registered in the United Kingdom. Company number 8096230

63/66 Hatton Garden, London, EC1N 8LE

editor's note

Hello and welcome to the latest edition of *Intelligent CISO* where we bring you a roundup of the trends and developments taking place across the cybersecurity market, on a global scale. We hear from several industry experts who offer their best practice advice on hot topics of interest.

This month's cover story explores how one of Germany's leading hospital operators is ideally placed to meet the needs of today and tomorrow whilst bolstering its reputation as a trusted, security-conscious healthcare group. Daniel Maier-Johnson, CISO at Asklepios, explains how it used VMware's products to ward off cyberattacks and become more aware and responsive to new threats. This can be found on page 51.

Another of our interesting stories this month takes a look at the insider threat. On page 36, we delve deeper into the findings of a recent Proofpoint study which shows businesses globally are losing around £11.4 million (US$15.4 million) every single year because of insider cyberthreats.

A hot topic featuring heavily in conversations across the industry is Identity and Access Management (IAM), and we explore this further on page 48. Craig Ramsay, Senior Solution Consultant, Omada, discusses the management of identities and their associated risk and how business leaders can strengthen their security strategies for the months to come.

Zero Trust is another leading trend raising its head across the industry and we hear from PJ Kirner, CTO and Co-founder at Illumio, who discusses security spending and strategy building as well as developing a robust Zero Trust approach to cybersecurity. This can be found on page 62.

On page 67, we focus on whether AI is the answer to the SOC's problems as Geert van der Linden, Cybersecurity Business Lead at Capgemini Group, suggests how SOCs can work smarter to lighten the load with technology.

To round off, we 'Go Phish' with John Smith, EMEA CTO, Veracode, who tells us about his career journey so far and how he likes to relax and unwind outside the office. Find out more on page 71.

I hope you enjoy the read and if you'd like to contribute to any upcoming editions, please do get in touch at alix@lynchpinmedia.com

Alix Pressley
Editor

Trend Micro blocked over 94 billion threats in 2021

Trend Micro has announced that its industry-leading threat intelligence infrastructure, Smart Protection Network (SPN), stopped 94.2 billion cyberthreats heading for consumer, government and business customers in 2021.

The volume of detections represents a 42% increase on the number of detections recorded in 2020. It revealed that attacks surged by over 53 billion in the second half of 2021 after Trend Micro blocked 41 billion threats in 1H 2021.

The threats were detected by more than 5 trillion threat queries, a 36% year-on-year increase from queries in 2020. Trend Micro's SPN leverages over 250 million sensors across the broadest attack surface globally to proactively protect organisations and individuals faster.

"Trend Micro detects threats across endpoints, mobile, servers, IoT/IIoT, home networks, messaging, network, web and cloud environments," said Jon Clay, Vice President of Threat Intelligence for Trend Micro. "That's a testament to our continuous effort to expand attack surface protections and improve our advanced detection technologies deployed to 500,000 commercial and government accounts and millions of consumer customers. But it also underscores the mounting threat from bad actors."

Despite a double-digit surge in detected cyberthreats from 2020 to 2021, Trend Micro blocked 66% fewer ransomware attacks over the period, reinforcing the theory that these threats are becoming more targeted. Another contributing factor in this decrease is that more ransomware attacks are being blocked in earlier stages before being deployed. Over 14 million attacks were proactively stopped in 2021 before they could impact customers.

IDC MarketScape report names BT as a leader in Managed Security Services in Europe

BT has been named as a leader in the *IDC MarketScape: European Managed Security Services 2022 Vendor Assessment* report. BT's security team provides solutions to consumers, governments and businesses around the world and protects the company's global network against around 200,000 cyberattacks per month.

The placement reflects BT's 'combination of pan-European network assets and proven experience and capabilities in security'.

BT was recognised for its ability to seamlessly integrate its security portfolio with wider network and cloud solutions and for its wider emphasis on security innovation and partnerships across leading academic and research institutions. Its recent investment in Safe Security was also highlighted, as its risk assessment and prediction capabilities were seen as becoming increasingly important, considering recent supply chain attacks, such as SolarWinds.

Last year, BT launched its transformational new cyberdefence platform 'Eagle-i', which incorporates AI to advance the speed and capability of its security operations. The *IDC MarketScape* report stated that the use of proprietary technology in Eagle-i and the platform's ability to draw on threat intelligence from BT's extensive European network infrastructure 'makes it hard to match precisely by other MSSPs (Managed Security Service Providers)'.

Australia agrees Cyber and Critical Technology Partnership with UK

UK Foreign Secretary, Liz Truss, has agreed a new Cyber and Critical Technology Partnership with Australia's Foreign Minister, Marise Payne.

The agreement seeks to strengthen global technology supply chains, ensure the UK's positive technology vision and to tackle malign actors who attempt to disrupt cyber-space.

The new agreement includes provisions to build greater resilience to ransomware among Indo-Pacific nations and sharpen legal sanctions against cyberattackers. It will also deepen practical co-operation on ensuring technology standards reflect the two countries' shared values.

UK Foreign Secretary, Liz Truss, said: "As champions of freedom and democracy, the UK and Australia are hard-headed in defending our values and challenging unfair practices and malign acts.

"In the battlegrounds of the future, cutting-edge technologies will be crucial in the fight against malign cyberactors who threaten our peace and security.

"That's why the UK and Australia have agreed a new cyber and technology partnership to ensure that liberal democracies shape the technology rules of tomorrow."

Signed by Truss in Sydney during her visit to Australia, the agreement will also support development of a 'network of liberty' that will deter cyberattacks before they happen and call out malign actors who perpetrate the acts.

The Ocean Race teams up with Acronis

Acronis, a global leader in cyberprotection with dual headquarters in Schaffhausen, Switzerland and Singapore, will be the Official Cyber Protection Partner of the iconic round-the-world sailing competition, The Ocean Race.

The partnership will be supported by Ingram Micro, a global distributor of innovative technology products and services, as the Official #CyberFit Partner, in line with the Acronis #TeamUp Programme.

"Acronis is proud to support The Ocean Race, which is committed to sustainable operations in all aspects of the race," said Jan Jaap Jager, Acronis CRO and Board Advisor. "Sports teams use Acronis Cyber Protect to optimise cybersecurity operations and make cyberprotection more efficient."

"Technology and innovation are at the heart of what we do at The Ocean Race and this has enabled us to continuously push the boundaries on how our sport is delivered to fans and partners worldwide for nearly 50 years," said Rik Roukens, Technology Director of The Ocean Race.

"With Acronis joining us as Official Cyber Protection Partner, we can continue to push those boundaries with the assurance of best-in-class data protection and Disaster Recovery systems."

illumio

Stop Ransomware. Isolate Cyberattacks. Reduce Risk.

Segment in minutes on your path to Zero Trust.

Real-time visibility and Zero Trust segmentation from Illumio allow you to see and secure your most important data and applications across clouds, containers, data centers and endpoints.

90%
Simpler
Eliminate manual network segmentation

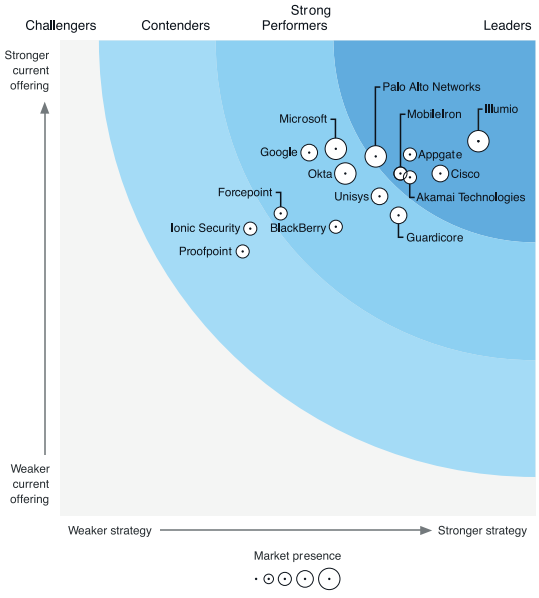
5x
Faster
Segment at the speed of business

100%
Confidence
Reduce risk and increase uptime

FORRESTER®

Illumio named a Leader in The Forrester Wave™ for Zero Trust

Highest scores in three primary categories: current offering, strategy and market presence.



Learn more at illumio.com

Customers in North and Latin America offered access to BlastShield

BlastWave, a pioneer in invisible software-defined perimeter solutions designed to protect critical infrastructure assets and applications, has announced a partnership with Brier & Thorn, a leading Managed Security Service Provider (MSSP). As a part of the agreement, Brier & Thorn will offer BlastWave's BlastShield solution to its global customer base across North America and Latin America.

"Partnering with Brier & Thorn opens so many doors for BlastWave and will allow us to support top technology customers across Latin and North America," said Tom Sego, CEO, BlastWave. "Working with Brier & Thorn's channel partners is mutually beneficial. We will allow users that scrambled to meet the remote and hybrid work requirements driven by the pandemic to significantly upgrade their performance and security posture from the flawed, legacy VPN stopgaps.

"BlastShield allows customers to quarantine their network and prevent malware spread and eliminate the annoying aspects of remembering usernames and passwords, while enforcing 100% Multi-Factor Authentication. We take Zero Trust security to a whole new level."

Brier & Thorn advises global leaders on their most critical IT risk management issues and opportunities including Global 500, global manufacturers, retailers, biotechnology and pharmaceutical companies, automobile manufacturers and financial services.

Safe Security and Infosys partnership to identify enterprise vulnerabilities

Safe Security, a global pioneer of cyber-risk quantification solutions, has announced a strategic collaboration with Infosys, a global leader in next-generation digital services and consulting.

Safe Security's SaaS platform, SAFE, combined with Infosys' capabilities in quantitative cyber-risk management will enable organisations to get an enterprise-wide view of overall cyber-risks, predict breaches using SAFE's proprietary algorithm and know the potential financial impact of each cyberattack before it occurs.

SAFE provides organisations with real-time visibility into their biggest cyber-risks. This is done by aggregating signals via APIs into a single dashboard, with actionable insights and potential financial impacts.

The insights gained from SAFE also provide a common language for discussing cybersecurity risks with board members, auditors and other internal and external stakeholders.

By combining these insights with Infosys' on going strategic guidance, joint customers will benefit from a more proactive cybersecurity approach.

Amir P. Desai, CIO, Molina Healthcare, said: "Prior to SAFE, we didn't have any centralised tool to monitor the security loopholes identified through configuration and vulnerability assessments, red teaming exercises, and security audits for compliance, for each technology stack across each of my business units and acquired businesses.

"With SAFE and Infosys' leadership in helping large organisations manage cyber-risk, we now have a real-time, data-backed and continuous view of exactly how secure our critical applications storing, processing and managing PHI are."

Help AG partners with Owl Cyber Defense to offer network protection

Help AG, the cybersecurity arm of Etisalat Digital and the region's trusted IT security advisor, has partnered with Owl Cyber Defense, a global provider of Edge security and Cross Domain Solutions (CDS), to offer high-assurance network protection and secure data transfers to critical infrastructure and OT environments.

A pioneer in data diode technology, Owl is the only solutions provider with over 20 years experience in cross domain solutions that are enforced with data diodes.

Some of the world's largest industrial and commercial organisations, including multiple US government and security agencies along with 90% of the country's nuclear power plants, trust Owl with the defence of their most sensitive digital assets.

Stephan Berner, Chief Executive Officer, Help AG, said: "As regional leaders in cybersecurity, Help AG deploys best-of-breed security technologies to design, implement and configure complex end-to-end security architectures unique to each customer, with a division dedicated to delivering world-class solutions for the OT space. Our partnership with Owl, a global pioneer in hardware-enforced cybersecurity products, perfectly complements our portfolio to offer a complete suite that elevates our customers to greater levels of protection."

Sheffield Hallam University partners with FDM Group to create 500 apprenticeship jobs

FDM Group, a professional services provider with a focus on technology, has announced its first ever apprenticeship programme, offering new joiners the opportunity to gain degree-level qualifications as part of an innovative training course.

Candidates will be given full vocational training in key IT roles alongside study as part of the government-approved level six (Bachelor of Science Degree) Digital and Technology Professional apprenticeship. After the initial training phase is complete, employees will then be able to specialise in key areas such as IT consultancy, software engineering, cybersecurity and data science. As part of FDM Group's commitment to diversity and inclusion, the apprenticeship programme will operate with a 50:50 gender split, with many candidates coming from under-represented backgrounds.

The initial stage of the programme has been developed in partnership with Sheffield Hallam University, with FDM expecting to sign additional agreements in London and with other universities across the country in the coming weeks.

The Sheffield Hallam course starts with a solid 12 weeks first term block, onsite at the university. The next seven terms have a study week in the middle of the term and then the ninth term is final exams. For the at-university study blocks (including the 12 weeks), FDM apprentices receive full salary and FDM subsidises their accommodation in Sheffield.

CELEBRATING 10+ YEARS OF TRUST...

ENABLING DIGITAL TRANSFORMATION

- AI Chatbots
- BI & Analytics
- Blockchain
- CRM / CEM
- ECM
- Robotic Process Automation
- Managed IT Services

SECURING DIGITAL TRANSFORMATION

- Digital Risk & Compliance
- Zero Trust
- Cloud & Application Assurance
- Digital Identity
- Data Protection & Privacy
- Managed Security Services

+971 52 456 1683
+971 4 3300 144
info@finessedirect.com
www.finessedirect.com

FINESSE

MENA | APAC | AMERICAS

450+ Professional Team | 350+ Enterprise Clients | 50+ International Awards | 10+ Global Locations | 20+ Nationalities

Threat intelligence is among the most sought-after security service for MSPs in META

The majority (93%) of Managed Service Providers (MSPs) across the META region are currently planning to add new services to their cybersecurity portfolio, where threat intelligence is among their top choices, along with managed detection and response and targeted attack discovery. These are the findings of a new Kaspersky report, *MSP market focus: IT security challenges and opportunities in the new normal*. As perceived competition in the market has risen since 2019, pricing, quality of protection and ability to offer additional services become key factors for choosing a cybersecurity vendor.

Cybersecurity is one of the most prominent areas of growth for MSPs, according to various industry experts. It presented the biggest opportunities for growth in 2021, together with remote workforce setup – with 65% of MSPs reporting security service revenue growth as a result.

As for threat intelligence, which was among the top interests of MSPs as revealed by the Kaspersky survey, 'It is a key aspect of security architecture that helps security and risk management technical professionals detect, triage and investigate threats', according to Gartner.

Among various threat intelligence services, the most interesting for MSPs across the META region according to the research is APT reporting (18%), which allows them to keep up-to-date with the most recent investigations, threat campaigns and techniques of APT actors. This is followed by threat data feeds (16%) and threat lookup (13%) that help to improve incident response. Other services that providers look for include malware analysis (31%), security assessment (40%) and targeted attack discovery (47%).

LogRhythm partners with SecLytics to deliver enhanced cybersecurity capabilities in Middle East region

LogRhythm, a company powering Security Operations Centres (SOCs), has partnered with SecLytics, a predictive threat intelligence solutions provider, to transform the security posture and streamline operations for SOC teams in the Middle East.

Under the accord, LogRhythm and SecLytics will work hand-in-hand to provide enhanced threat intelligence capabilities and high-performance analytics, to mitigate new and evolving risks in the region. Through the collaboration, LogRhythm and SecLytics will enable organisations in the Middle East to seamlessly deliver Digital Transformation and protect their end-users with aligned early threat detection and response solutions.

"Data breaches in the MENA region are reported to have reached an average cost of around US$6.5 million, which is well above the global average incident cost of near US$4 million," said Mazen A. Dohaji, Vice President, India, Middle East, Turkey and Africa (iMETA) at LogRhythm.

"Cybersecurity risks in the Middle East are becoming increasingly sophisticated and this is causing organisations in the region to suffer notable losses. Overcoming new threats requires cybersecurity organisations to bring together their capabilities to build a protected threat environment for businesses in the region. Our collaboration with SecLytics is building a security-first future in the Middle East."

Saeed Abu-Nimeh, Co-founder and CEO, SecLytics, said: "We are working with LogRhythm to transform cyber resiliency in the Middle East and enable organisations to expand their applications and services without risk."

New KnowBe4 feature enables peer comparisons with security culture benchmark

KnowBe4, the provider of the world's largest security awareness training and simulated phishing platform, has announced it has launched a new Industry Benchmark feature that allows organisations to compare their security culture with others in their industry, creating an opportunity to evaluate key information around security culture with meaningful data. This feature is available via benchmark comparison data for KnowBe4's Security Culture Survey (SCS).

KnowBe4's science-based SCS helps security professionals tailor training to address proficiency gaps and weaknesses, as well as monitor the impact that their security awareness training programme has on improving their users' knowledge and sentiment to security awareness over time. The SCS provides an overview of the seven dimensions that make up an organisation's security culture and an overall security culture score for the organisation. SCS Benchmarking can be utilised to track how an organisation's culture changes over time relative to a specific industry.

"This new feature provides our customers with the ability to discover how their security culture stacks up across the seven security culture dimensions from their baseline assessment

compared to an all-industry average or their specific industry," said Stu Sjouwerman, CEO, KnowBe4. "It will allow for further analysis, awareness and proficiency when it comes to assessing an organisation's overall security culture. KnowBe4 is advancing its capabilities related to security culture to help enhance our customers' security posture."

More C-suite engagement needed in 2022 to mitigate cyber-risk

Trend Micro, a global leader in cloud security, has published new research revealing that persistently low IT/C-suite engagement may imperil investments and expose organisations to increased cyber-risk. Over 90% of the IT and business decision-makers surveyed expressed particular concern about ransomware attacks.

Despite widespread concern over spiralling threats, the study found that only around half (57%) of responding IT teams discuss cyber-risks with the C-suite at least weekly.

"Vulnerabilities used to go months or even years before being exploited after their discovery," said Eva Chen, CEO of Trend Micro.

"Now it can be hours, or even sooner. More executives than ever understand that they have a responsibility to be informed, but they often feel overwhelmed by how rapidly the cybersecurity landscape evolves."

Fortunately, current investment in cyber initiatives is not critically low. Just under half (42%) of respondents claimed their organisation is spending most on 'cyberattacks' to mitigate business risk. This was the most popular answer, above more typical projects like Digital Transformation (36%) and workforce transformation (27%). Around half (49%) said they have recently increased investments to mitigate the risks of ransomware attacks and security breaches.

However, low C-suite engagement combined with increased investment suggests a tendency to 'throw money' at the problem rather than develop an understanding of the cybersecurity challenges and invest appropriately. The study follows previous Trend Micro research revealing a worrying cybersecurity disconnect between business and IT leaders – perpetuated by self-censorship from cyber experts and disagreements over who is ultimately responsible. ◆

Discover the true hidden cost of Microsoft 365's default security features.

Don't let 'default' define your email protection.

proofpoint.

https://www.proofpoint.com/uk/hiddencostoffreeo365

THE HIDDEN COSTS OF FREE

WHY MICROSOFT 365'S NATIVE SECURITY FEATURES MAY NOT BE THE VALUE THEY SEEM

PRESENTED BY

proofpoint.

Introduction

As more and more organisations make the move to Microsoft 365, the software giant is pitching the platform as a way to consolidate security, compliance and e-discovery. It promises advanced threat protection, data protection and an online archive that's all about privacy and meeting robust data-retention requirements. And it's all included in your 365 subscription plan. How could anyone turn down that offer?

It may seem like a no-brainer. Why spend more money on third-party email security or archiving when it comes as part of your Microsoft licence? Aren't all email, cloud and compliance solutions pretty much the same?

The answers to those questions aren't as simple as they seem. Microsoft security might be fine for some purposes. But it could also lead to problems and cost more than you expect. That's because not all advanced threat protection or compliance archiving solutions are created equal. Think about the differences between a camping tent and a house. Both can keep you dry during a sudden rain shower. But in a winter storm with gale-force winds, only one of them will make a good shelter.

In the same way, an advanced email security solution can provide better security and compliance defences in today's stormy cybersecurity environment. Microsoft 365's native offerings just may not offer the level of security and compliance you need. ◆

DOWNLOAD WHITEPAPERS AT: WWW.INTELLIGENTCISO.COM/WHITEPAPERS

THE KNOW-HOW YOU NEED TO POWER THE MOST CHALLENGING ENVIRONMENTS

PRESENTED BY

Server Technology
A brand of legrand

EXECUTIVE SUMMARY

As data centers address more expansive and unique challenges, so too must their power distribution equipment meet those performance needs.

Server cabinets and racks, even individual server units, need to be designed for maximum adaptability to the ever-changing power consumption requirements of their unique and demanding environments.

Whether dedicated to supercomputing or artificial intelligence, data centers are by their very nature unique in form factor and physical architecture.

Sometimes they'll fit into an existing building on campus, with a retrofit of new infrastructure to support the additional demands placed on the power and cooling systems of the facility. Other times they're installed in an entirely new facility designed expressly for housing the machinery.

In both instances, administrators must find custom solutions for delivering power, cooling, networking, and so forth.

On the other hand, edge computing is designed to put applications and data closer to devices – and their users.

But it brings a different set of challenges than the massive data centers used in supercomputing and AI applications. Space is a significant one in many cases; smaller enclosures mean even less space for the power distribution equipment.

Because edge computing takes place remotely, you need to validate remote connectivity and possibly remediate any issues.

Data Centers Require Power And Lots of It

It's as simple as that.

The design of data centers has always required solving how to feed their power needs and distributing the electrical power once it's in the facility. ◆

RAPID7

INSIGHT PLATFORM

Shut down attacks with clarity and confidence.

Cloud Security

Vulnerability Risk Management

Application Security

Detection & Response

Threat Intelligence

Orchestration & Automation

Managed Services

Secure Everywhere

rapid7.com

Why cyber-risk mitigation should be top priority for every organisation

ANTHONY J. FERRANTE, GLOBAL HEAD OF CYBERSECURITY AT FTI CONSULTING, OUTLINES HIS TOP 10 CYBERSECURITY PREDICTIONS FOR 2022.

The evolutionary nature of cyberattacks is well known. Cyber actors continually improve on already sophisticated techniques and keeping pace is a never-ending challenge. With a threat landscape that has never been as vast or dispersed due to a hybrid workforce, cyber-risk mitigation should be the top priority for every organisation across the globe. Based on how quickly things change, predicting what is to come is difficult, but assessing what has already occurred can be a helpful indicator for preparations. Here are 10 predictions that the global FTI Cybersecurity team expects to see in 2022.

1. Regulatory hammers will fall

- **Background:** Cybersecurity-focused regulation, specific to government agencies and their related entities, was a focus in 2021. In October, the Department of Justice announced the Civil Cyber-Fraud Initiative, which will 'utilise the False Claims Act to pursue cybersecurity related fraud by government contractors and grant recipients.' A month later, the Biden Administration issued a mandate requiring 'federal agencies patch hundreds of cybersecurity vulnerabilities that are considered major risks for damaging intrusions into government computer systems.'
- **Prediction:** Between the increase in regulation and public demand for organisations to do all they can to protect sensitive user information, expectations for proper cybersecurity measures to be implemented are high. The private industry tends to follow suit with actions and guidelines established by the government, so it's safe to assume that similar basic cybersecurity requirements, at a minimum, will expand beyond the public sphere and organisations will face consequences for failing to comply.

2. Critical infrastructure will remain a significant target

- **Background:** The consequences of the critical infrastructure sector suffering a cybersecurity incident are so dire that the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI), release periodic reminders to stay vigilant. The complex nature and connectedness of digital and physical assets in critical infrastructure, combined with reliance on legacy equipment, make proper cyber-risk mitigation co-ordination a challenging task.
- **Prediction:** The proliferation of Internet of Things (IoT) devices within the Operational Technology (OT) space is growing rapidly and the efficiency they provide is often prioritised over security. This afterthought mentality carries

significant implications for sectors where IoT devices have been widely deployed, such as healthcare and the electrical grid. Cyber actors are well aware of the vulnerabilities and until protecting this industry is prioritised, it will continue to be targeted.

3. Third-party cyber-risk will be the biggest problem organisations face

- **Background:** At the end of 2020, US federal agencies and high-profile companies were hit with a major advanced persistent threat cyberattack. The breach occurred via a compromised and weaponised version of a software update from a connected third party. This type of prolific and widespread attack created a roadmap for other cyber actors to replicate in future malicious campaigns.
- **Prediction:** The increased reliance of organisations outsourcing to vendors as a result of a remote workforce has extrapolated an already prevalent threat in third-party cyber-risk. With more access points for cyber actors to exploit and organisations unsure how to manage and protect their entire digital ecosystem, cyber actors will continue to use connected parties as access to their main target.

4. Data ethics will play a prominent role in organisational strategy

- **Background:** As consumers request to further understand how their personal information is used, stored and shared, organisations are making efforts to adequately respond, especially around biometrics, such as facial recognition technology. This is especially true for organisations interested in implementing and leveraging Artificial Intelligence.
- **Prediction:** The ethics surrounding personal information and data will play a major role in the viability of organisations in 2022. Those who make protecting this information a priority will be viewed favourably, while those who choose to do the opposite will remain at risk to damaging cyberattacks, as well as consumers choosing to take their business elsewhere.

5. Sophisticated and targeted mobile malware attacks will become more common

- **Background:** Pegasus spyware made major headlines in 2021, as it was used to collect information on individuals without their knowledge or consent. The revelation that high-profile individuals, journalists and human rights activists were specifically targeted by nation-state actors using sophisticated mobile malware was eye-opening and cause for alarm.
- **Prediction:** These types of cyberattacks will become more prevalent and widespread as similar perpetrators continue to refine and evolve their capabilities to evade detection. Knowing that surveillance can be conducted without interaction from the target will lead to nation-state actors further relying on these types of tools to gather valuable intelligence and influence strategic objectives in their favour.

6. Nation states will access a digital passport or tracing app database

- **Background:** Depending on the country, everyday tasks, like entering a grocery store, may require displaying proof of receiving the COVID-19 vaccine through an approved app. Other jurisdictions mandate opting into location tracking on mobile devices so that tracing infected individuals is made possible. Both scenarios present situations where sensitive information is captured and stored.

netskope

Redefining cloud, network and data security

The Netskope Security Cloud provides unrivaled visibility and real-time data and threat protection when accessing cloud services, websites, and private apps from anywhere, on any device.

netskope.com

- **Prediction:** COVID-19 has created plausibly justifiable ways to track people and collect information about them. The nature of this information, vaccination status and location data points, is valuable to nation states who can use it for blackmail or leverage at a later date. Apps and their databases are often spun up quickly, especially in this instance, without considering the cybersecurity risks or data protection threats and subsequently, a nation state will breach a database as a result.

7. Cryptocurrency will face increased oversight

- **Background:** The FBI released an announcement in November 2021 warning of 'fraudulent schemes leveraging cryptocurrency ATMs and Quick Response (QR) codes to facilitate payment'. A lack of federal regulation regarding cryptocurrency transactions has led to state-specific laws with varying levels of requirements and calls for uniform legislation to mitigate the spread of cybercrime.
- **Prediction:** As cryptocurrency companies become more mainstream and established, cyberattacks targeted at these entities will increase. The combination of cryptocurrency ATMs becoming more popular and the anonymous nature of transactions many states permit will fuel the success of cyber actors. In response, regulation regarding cybersecurity, Know Your Customer standards, anti-money laundering and fraud can be expected to increase.

8. Soft targets will be heavily attacked

- **Background:** Soft targets, like schools, are organisations that notoriously have weak security protections in place for reasons like lack of skilled staff and budget. There was a record number of cyberattacks against schools in 2020, perpetuated by a shift to virtual learning, accompanied by additional entry points for cyber actors to exploit. These attacks came in various forms, from 'ransomware attacks, class interruptions on virtual learning platforms, phishing emails and identity theft'.
- **Prediction:** Due to cybersecurity protections of soft targets being largely unsophisticated and also lacking resources required to identify and mitigate threats, cyber actors will continue targeting these groups. The low infiltration cost and ease of entry against weak defences suggest that cyber actors will attack soft targets and turn their sights to more profitable campaigns, such as ransomware or theft of sensitive information.

Anthony J. Ferrante, Global Head of Cybersecurity at FTI Consulting

9. More cyberattacks will be executed via commoditised devices

- **Background:** There are an estimated 13.8 billion IoT devices in use worldwide, a number that is predicted to surpass 30 billion by 2025. This includes products like smart thermostats and smart refrigerators, which are becoming more commonplace. The influx of IoT manufacturing means these devices are becoming more accessible and cheaper to acquire.
- **Prediction:** Cyber actors are skilled at analysing a situation and determining how it can be exploited to their advantage. Regarding commoditised devices, there are endless options for cyber actors to infiltrate and compromise. In 2022, cyberattacks leveraging these connected products, ranging from accessing sensitive information stored on a home network, to spying on targeted individuals, will increase.

10. Cyberattacks will enter the final frontier

- **Background:** There are roughly 7,500 active satellites orbiting Earth. Similarly to Operational Technology, satellites are often viewed as being 'unplugged' from the Internet and considered protected from cyberattacks. However, access has changed since many of the satellites were launched.
- **Prediction:** IoT devices are more commonly being used to communicate with satellites. As previously mentioned, these devices create entry points that cyber actors can exploit and then establish a foothold, escalate privileges and ultimately gain control of the satellite. This is a common attack progression and it can be expected that cyber actors will replicate this technique with devices not previously considered, like satellites, in 2022. ◆

LUMU TECHNOLOGIES SURVEY REVEALS CYBERSECURITY INVESTMENT PRIORITIES

Enterprise CISOs will have a lot on their plate in 2022 as they continue to grapple with securely connecting a remote workforce while addressing other pressing initiatives to protect their organisation from an evolving cast of threat actors. To better understand where and how CISOs plan to prioritise their investments this year', Lumu Technologies recently conducted its second annual survey of 300 cybersecurity leaders across North America and has compiled the results into an infographic.

For the second year running, Lumu polled CISOs and cybersecurity leaders on the projects they consider most urgent and compiled their answers in its 2022 CISO Priorities Flashcard.

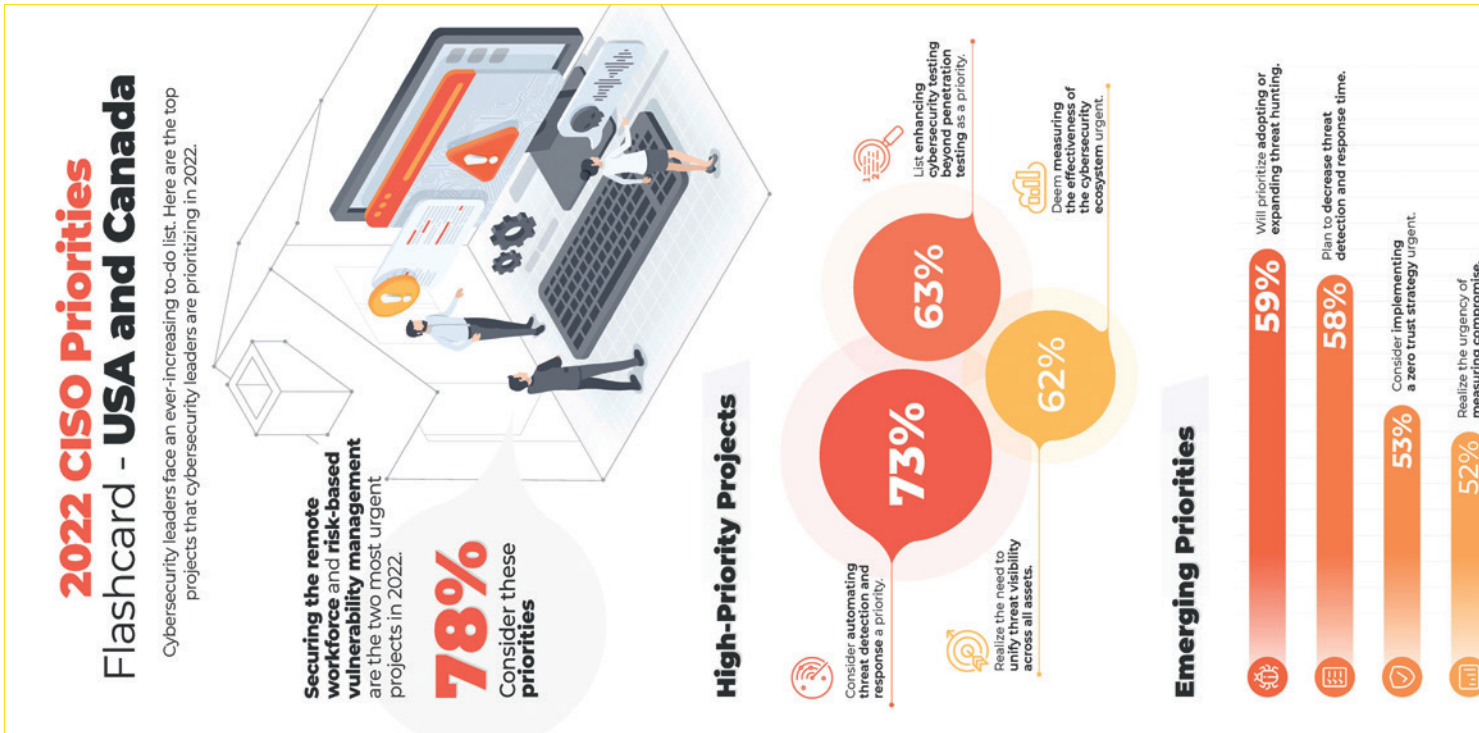
Among the many initiatives available for their consideration, here are some of the highlights:

The remote workforce

As businesses went remote in 2019, cybersecurity teams scrambled to secure users who left the security of the perimeter by going remote. Consequently, in 2021 94% of CISOs noted securing their remote workforce was an 'absolute priority' or 'priority'.

In 2022, the response is more muted from US CISOs. A total of 78% of CISOs regard securing the remote workforce as a priority, making it the top priority for the second year running. While it can

> Demand for cybersecurity talent is only increasing.



be assumed that CISOs addressed the initial impact of those cohorts starting to work from home, remote workers remain an ongoing concern. Under hybrid work models, devices moving in and out of perimeter defences represent new challenges and vulnerabilities.

Facilitating proficient day-to-day cybersecurity operations

In 2022, many top priorities concern the ease of cybersecurity operations. Automating threat detection and response (78%) and unifying threat visibility across all assets (62%) are some of our respondents' top priorities. These measures indicate that tools which make the SOC team's work more automated and more efficient are getting precedence. Demand for cybersecurity talent is only increasing. Efforts that help operators with their daily tasks not only make the most of an expensive resource but improve staff retention.

The cybersecurity big picture

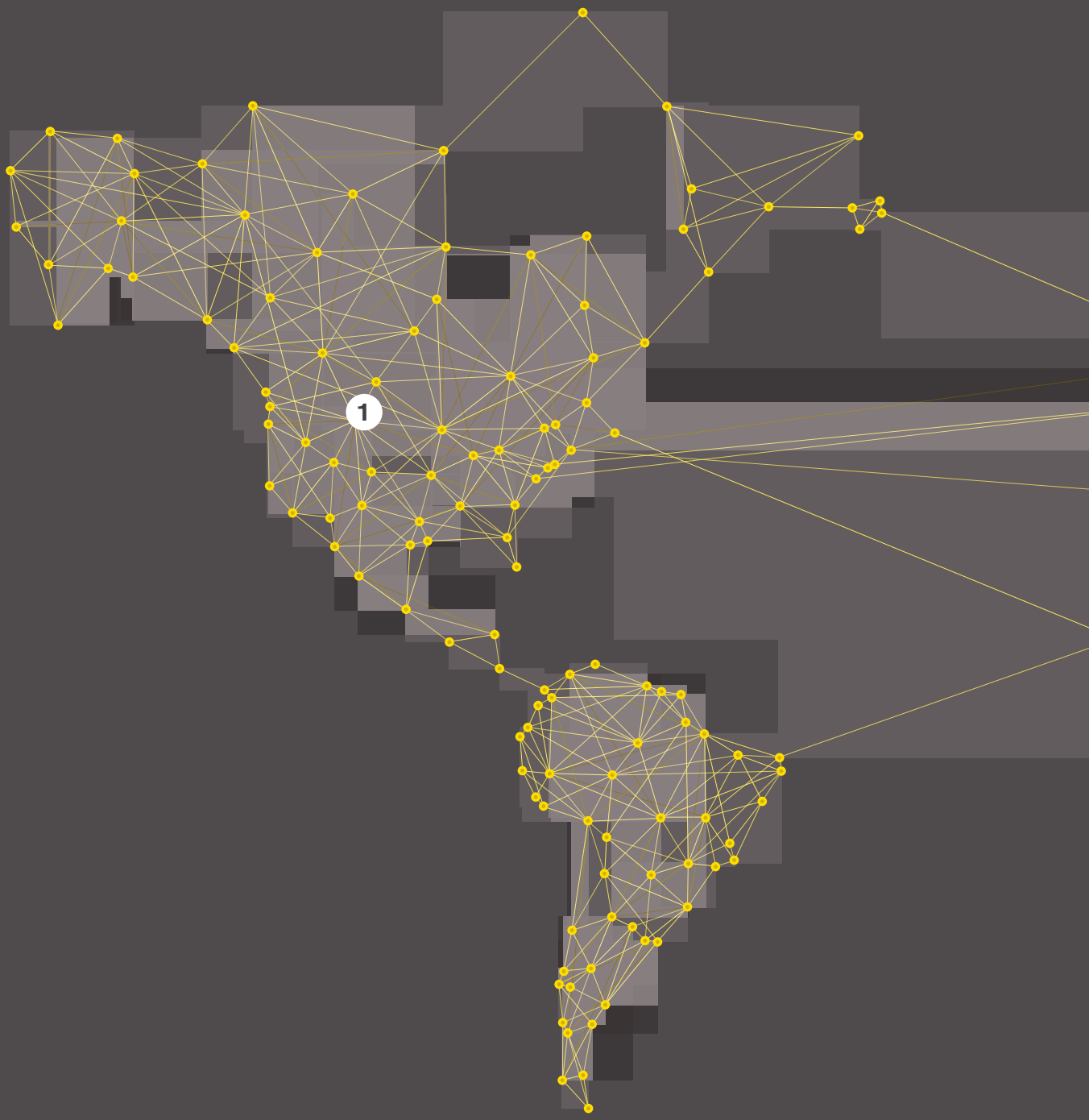
Improving the cybersecurity posture as a whole is at the forefront of CISOs' minds. Enhancing cybersecurity testing beyond penetration testing (63%) and measuring the effectiveness of the cybersecurity ecosystem (62%) are being prioritised in 2022. With so many tools, projects and methodologies to choose from, subjectively testing the system and its components is key. CISOs are looking to spend their budgets intelligently and get evidence of their performance that they can take back to their board.

Supply chain surprise

In 2021, supply chain attacks dominated the headlines, with the Kaseya and SolarWinds attacks at the forefront. Sophisticated attackers are looking to exploit vulnerabilities in pipelines and packages (such as log4j) to compromise organisations lower down in the supply chain. That's why it may come as a surprise that only 49% of cybersecurity leaders consider supply chain risk assessment a priority. In an ideal world, this should be a key component of any organisation's due diligence practices.

The SOC team is here to stay

CISOs are least interested in outsourcing cybersecurity operations (17%). Smaller businesses without a CISO or cybersecurity staff might acquire the help of a third party. However, organisations with mature information security stacks recognise the reality that cybersecurity is not just bought but operated. CISOs are committed to the constant measurement and improvement of their cybersecurity operations. ◆

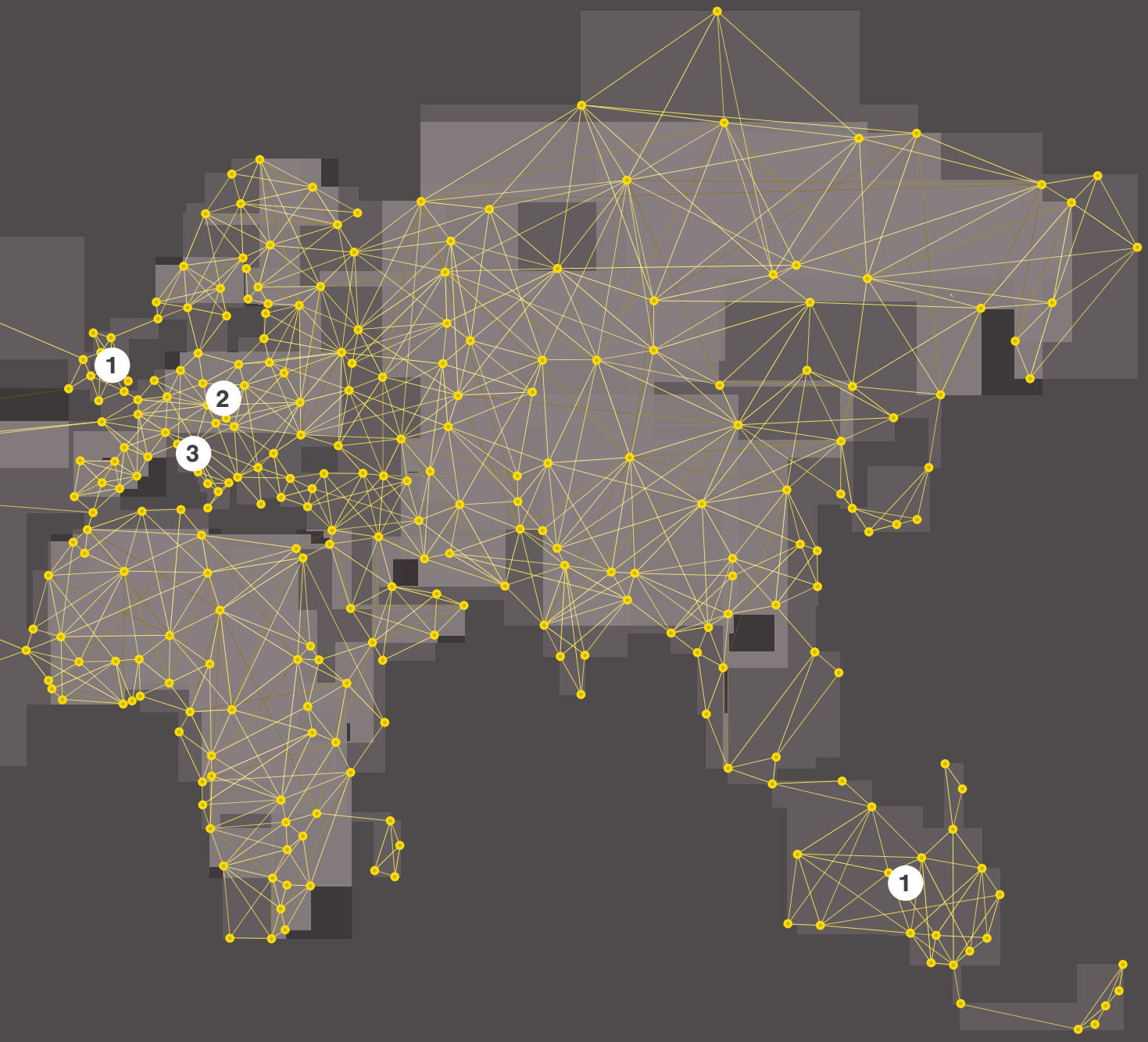


1 UK, US & AUSTRALIA

Cybersecurity experts from the UK, US and Australia have issued a joint cybersecurity advisory warning of the 'growing wave of increasingly sophisticated ransomware attacks' which could have 'devastating consequences'.

2 EUROPE

Several European oil and transport companies have fallen victim to a cyberattack, leaving dozens of terminals across Europe with IT systems severely disrupted. Oiltanking in Germany, SEA-Invest in Belgium and Evos in the Netherlands were targeted.



3 SWITZERLAND

Aviation services company, Swissport International, has disclosed a ransomware attack that has impacted its IT infrastructure and services, causing flights to suffer delays. The Swiss company provides services for cargo handling, security, maintenance, cleaning and lounge hospitality for 310 airports in 50 countries. It handles 282 million passengers and 4.8 million tons of cargo every year, making it a vital link in the global aviation travel industry chain. A tweet from the company notes that the attack has been largely contained and systems are being restored to bring services back to normal.

4 GLOBAL

KP Snacks has fallen victim to a ransomware attack which could lead to a shortage of supply until the end of March, the company has said. The attack appears to have been caused following a breach of KP's internal network, with attackers gaining access to and encrypting sensitive files, including employee records and financial documents.

THE WORLD'S CRITICAL INFRASTRUCTURE IS UNDERGOING TREMENDOUS CHANGE.

Connected as never before.

Our electric systems. Water utilities. Oil and gas infrastructures. Chemical, food, and pharmaceutical manufacturing. All, digitally transformed. Introducing new complexity to operations and industrial control systems, and new risks.

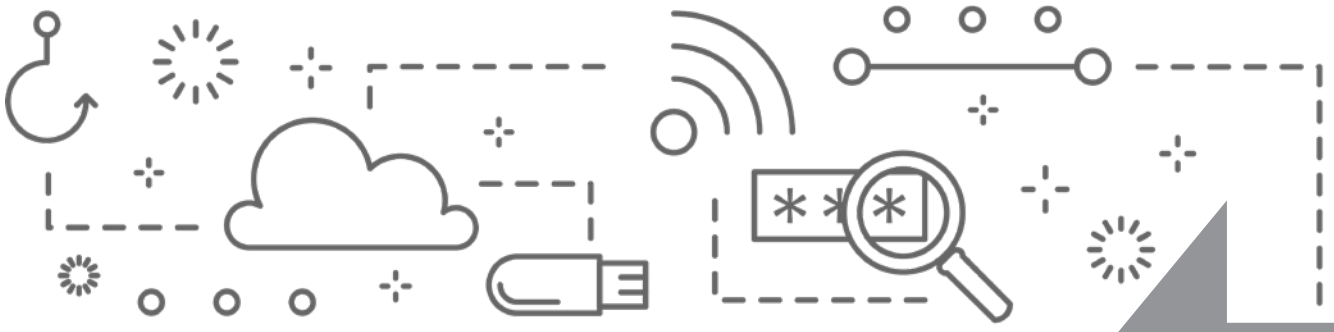
Who do you trust to defend critical assets from threat groups who specialise in operational technology?

An ally who knows it even better than them. Dragos.

For more information visit: dragos.com

Founded by the experts trusted to investigate and analyse the most significant cyberattacks on operational technology in history. Dragos is the largest, most experienced team in the industry – with proactive and reactive service teams that understand your specific OT environment.

DRAGOS



WHAT ARE THE TOP SECURITY THREATS TO ORGANISATIONS IN THE APAC REGION?

FS-ISAC, a global cyber-intelligence sharing community focused on financial services, has announced that ransomware and supply chain attacks, as well as the resurgence of banking trojans and distributed denial of service (DDoS) attacks, are the top cybersecurity threats to financial institutions across the Asia Pacific (APAC) region.

2021 has seen a steady rise in cross-border cyberattacks perpetrated by increasingly sophisticated threat actors. Based on FS-ISAC member intelligence sharing, open-source intelligence and insights from local financial firms and other sources, the Financial Services Information Sharing and Analysis Center's (FS-ISAC) *2021 Cyber Trends and Threats Review* sheds light on current strategic trends in financial services and cybersecurity and offers critical insights into the most salient cyberthreats facing the APAC financial services industry today.

The review also highlights key guidance for how to prepare for emerging cyberthreats in 2022.

"As digitalisation of financial services across the APAC region takes place at record speed, firms should be aware of the accompanying pitfalls and take steps to mitigate them," said Christophe Barel, Managing Director for APAC, FS-ISAC.

"In particular, as the region's digital shift takes place amid organisational challenges and an under-supply of cybersecurity talent, firms may face the risk that digital expansion could outpace their capacity to adequately protect themselves from emergent cyberthreats.

"Safeguarding against these threats will require the collective wisdom of the entire industry, with intelligence sharing as a core pillar."

Current cyberthreats are converging with recent trends in financial services such as the wholesale move to cloud, the emergence of new FinTech players competing against traditional financial institutions and mainstream adoption of cryptocurrencies.

As Financial Institutions (FIs) have had to quickly expand their IT infrastructure to stay competitive, some have found that their cybersecurity apparatus has not scaled up at the same pace.

The *FS-ISAC 2021 Cyber Trends and Threats Review* also identified other significant trends facing the region, including the strengthening of regulatory oversight of cyber-risk management, organisational challenges to threat response and an acute cybersecurity talent shortage.

As cybersecurity becomes a board-level issue because of the existential risks cyberattacks can pose, financial firms must re-imagine cybersecurity policies and procedures for a new era where the industry is hyperconnected and cyberthreats know no bounds.

"In 2021, third-party risk and ransomware continue to dominate the cyberthreat environment, while the resurgent threats of DDoS and trojans have also reared their heads. Sharing intelligence both globally and among members in the region can help firms understand not only new and emerging tools, techniques and procedures used by cybercriminals but also best practices on how to defend against them," said Barel.

The start of 2022 represents a very different cybersecurity climate to that of even two years ago. As businesses both big and small continue to navigate the new normal, the rise of Digital Transformation heralds a brand new world, characterised by increasing innovation and simultaneously, rising threats.

While some priorities around what is needed to meet customer and business needs will shift, what will always remain is a focus on security for APAC businesses.

Organisations will continue to face rising instances of data breaches and cyberattacks, along with the challenges of a hybrid workforce and managing legacy systems. To address this, security must remain a priority for information and technology leaders.

A greater need for a hybrid workforce, mobilised through the use of digital technologies, brings new challenges for businesses. Hybrid workplaces mean an increasing number of access points for malicious actors, contributing to the 56% of SMBs surveyed by CISCO in Asia Pacific who have experienced rising breaches.

With a globally mobile workforce, traditional security systems designed for a static workforce are no longer appropriate to keep sensitive information safe.

The solution is found in the adoption of digital identity management platforms and Zero Trust architecture which put the user at the centre of security.

Investing in biometric identification provides a unique form of identity access, putting users at the centre of their logins in a way that can't be replicated by malicious actors.

Adopting a Zero Trust architecture also helps restrict access controls to applications, networks and data by different groups of staff members or external stakeholders.

This provides a more comprehensive overview of what data is accessible by whom in the process. The benefit is a comprehensive solution minimising where points of attack can occur.

With a nearly 13% increase in the volume of cybercrime reported within Australia alone in 2021, business leaders must continually invest in stronger and more resilient systems.

They must also ensure none of the applications or programs they currently use contain any potential vulnerabilities.

Ongoing monitoring is key. Setting procedures in place to constantly monitor and re-evaulate every application and program used will help businesses identify programs no longer in use so they can remove them from their systems.

Having these procedures in place will also provide visibility into programs that need regular patching, to minimise instances where malicious actors can use these programs as potential back doors to facilitate cyberattacks.

JAMES ROSS, ANZ REGIONAL VICE PRESIDENT OF FORGEROCK

Finally, APAC organisations are experiencing an increase in the number of ransomware incidents and identity breaches. In Singapore, the rise of the pandemic saw ransomware incidents dominate the cyber landscape, and within Australia, there was a 30% increase in data breaches compared to 2020. While greater protections, monitoring and tech stack upgrades can help to mitigate this, investing time in building employee and customer awareness around threat management is equally important.

The *2021 ForgeRock Consumer Identity Breach Report* found that passwords and usernames (often shared across multiple platforms and websites) resulted in a 450% increase in cyberattacks. While not an uncommon practice, users fail to recognise the threat behind shared passwords and as a result, the lack of security can result in crippling losses.

Updated security policies and practices to encourage the use of login methods that require Multi-Factor Authentication will be crucial to minimising instances of breaches occurring this way. APAC is facing an increasing number of security threats.

With the way we work and how we utilise online services constantly shifting, businesses need to ensure cybersecurity is top of mind as they implement new services for customers and employees alike.

By getting into the habit of reviewing legacy systems and implementing more secure login methods like Multi-Factor Authentications, APAC businesses can help minimise instances of cyberattacks occurring.

The last two years have seen massive change in the cybersecurity landscape, largely driven by the pandemic and geopolitical pressures. At the same time, we've found some things have stayed the same.

According to NTT's 2021 *Global Threat Intelligence Report*, ransomware continues to be one of the most damaging forms of cybersecurity threats, with the finance industry the most attacked due to its large payoff. While we don't see these trends diminishing in the APAC region, we are seeing some new trends.

Increased disruption to the supply chain

Over the last few years, increased disruption to the supply chain has resulted in greater cyber-risk and vulnerability to back-end systems. The attack on Colonial Pipeline forced the company to close down operations and freeze IT systems, temporarily halting the supply of fuel and gas across the east coast of the United States.

More recently in Australia, Frontier Software, one of the largest cloud-based payroll providers was significantly impacted by a cyber event, resulting in many reliant organisations being forced to activate their Business Continuity and Disaster Recovery plans. These examples demonstrate that as businesses rely more on technology, the supply chain is an increasingly popular way for threat actors to either gain an entry point or cause significant disruption.

Manufacturing and healthcare experiencing larger volumes of cybersecurity threats

Criminal groups utilising ransomware do particularly well when they increase the pressure of decision-making and we see this happening in the healthcare and manufacturing sectors.

The healthcare industry's cyber maturity score in particular, continues to lag behind in APAC, sitting at 0.60 compared to the global average maturity level of 1.02 out of a top score of five.

While the manufacturing industry has a score of 1.98 compared to the global score of 1.21, it was the second most attacked in APAC, showing there are still significant vulnerabilities that can be exploited.

This is a stark reminder of the threats and potential impact that are caused by rapid Digital Transformation in critical industries not adequately addressing security.

Governments taking an active interest with the aim of increasing cybersecurity and business resilience

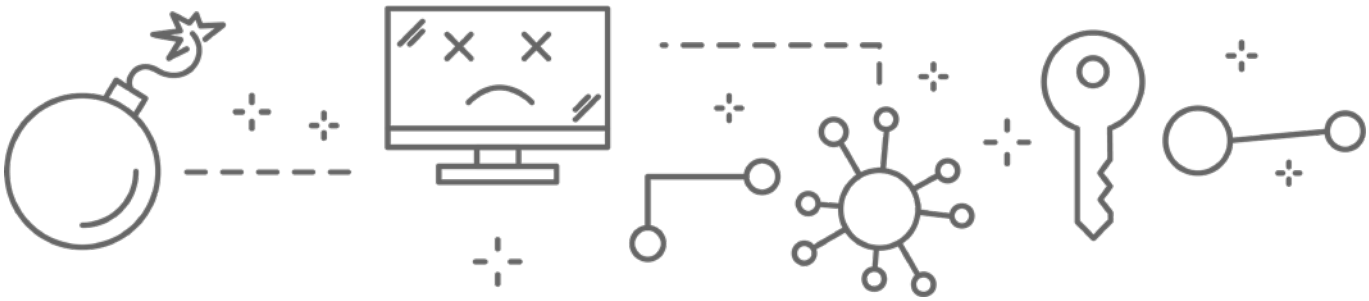
We are beginning to see many governments take an active role in cybersecurity policy, threat detection and prevention measures. The Australian government is on the cusp of passing the Critical Infrastructure Bill, which will allow the federal government power to assist or actively intervene in the security response of private organisations if required.

It will also increase the obligations around reporting and implementing essential cybersecurity practices.

With this new legislation, the very definition of 'critical infrastructure' is being expanded from four to 11 sectors including, utilities, health, food, transport and data storage.

It's great to see the government taking this up as an important initiative as it highlights the important collaborative role both industry and government have to play, with the dividend being an exciting digital future that we can rely on and trust in.

JOHN KARABIN, SENIOR DIRECTOR OF CYBERSECURITY, NTT AUSTRALIA



The pandemic has permanently altered the cybersecurity landscape, bringing with it a new set of threats and challenges to overcome.

While businesses were quick to adopt new technologies and accelerate Digital Transformation, they have been left exposed to cybercriminals who sought to exploit weaknesses for steep financial gains.

As leaders look to navigate new technologies, systems and processes to protect themselves from threat agents, I explore the top cybersecurity threats facing organisations across APAC today that require urgent attention.

Misconfiguration of Active Directory will continue to experience high volumes of ransomware attacks

Ransomware trends will continue to come and go as operators find new entry points and shift tactics to launch large-scale security attacks. But regardless of how tactics change, Active Directory (AD) will remain the go-to target as it's simply too lucrative for adversaries to pass up.

Threat actors will continue to leverage misconfigured AD to move laterally, escalate privileges, and create the same chaos experienced by some of the world's largest companies including SolarWinds and MSFT Exchange.

To secure the AD environment, organisations across APAC must patch and secure every configuration that is known to be exploited while remaining vigilant in the identification of new entry points. Put simply, AD must be secured and maintained 24/7. Without this level of commitment, multiple breaches should be expected in 2022.

Securing your hybrid workforce

With the rise of hybrid work, it will become even more difficult for organisations to protect enterprise data as employees constantly move from their homes to the office, connect to public Wi-Fi at the local coffee shop, and access enterprise information on their mobile devices while commuting.

This means businesses must now continuously monitor and verify every attempt to request access to data at all levels, whether that happens through a device, app, user or network attempting connection. Without this level of security, visibility and segmentation, attackers can leverage vulnerabilities in the environment, move laterally and infect other assets. While the adoption of a Zero Trust model doesn't happen overnight, it can play a vital role in an organisation's overall cybersecurity strategy.

SCOTT MCKINNEL, ANZ COUNTRY MANAGER, TENABLE

Collaboration is key to addressing critical infrastructure threats

As seen throughout the year, attacks on critical infrastructure environments can have dire consequences, not only for a business but society in general. Facilities are increasingly interconnecting their Operation Technology (OT) and IT networks to drive innovation. But this convergence has rapidly expanded the attack surface and increased the number of attack vectors. A lack of good cyber-hygiene within OT infrastructures has set up critical infrastructure environments to be high-value targets for cybercriminals.

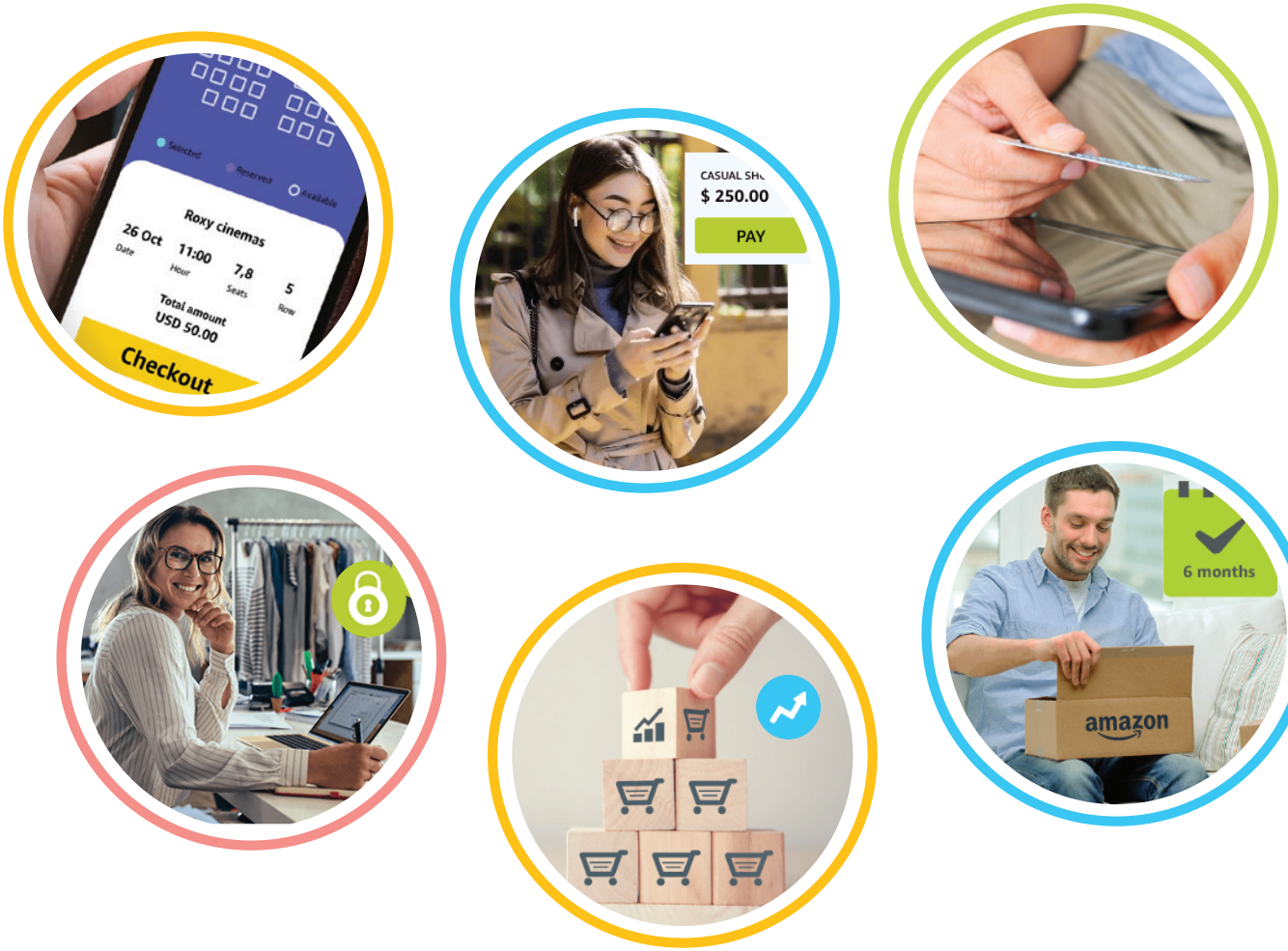
This calls for greater public and private sector collaboration to ensure baseline cybersecurity requirements are grounded in consensus-based, international standards. The establishment of best practices including the assessment of risk and collaborative response capabilities will play an integral role in strengthening the ability of industry and government to prevent even the most advanced attacks. ◆

As seen throughout the year, attacks on critical infrastructure environments can have dire consequences.

Secure, Seamless and Convenient

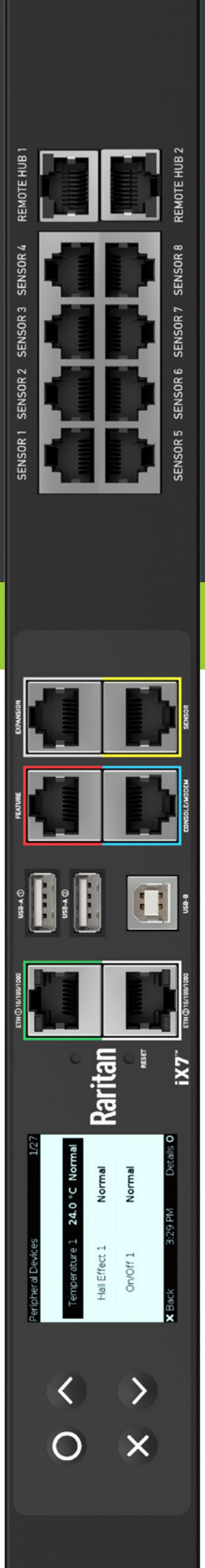
Provide your customers with the ultimate online shopping experience in the UAE, KSA, Egypt, Jordan, Lebanon, Qatar, Kuwait and Oman.

Local awareness, global know how



amazon payment services

Find out more



Raritan®
A brand of legrand®

SMART RACK CONTROLLER

AN INTELLIGENT SENSOR MANAGEMENT SOLUTION

Raritan's Smart Rack Controller is your central connection point for environmental monitoring, asset location, physical access, and other monitoring and security sensors.

BENEFITS OF THE SMART RACK CONTROLLER:

- Save time and money on asset tracking and cooling costs
- Easily retrofit and connect existing locations and infrastructure
- Ensure uptime by monitoring racks for hot spots and receive proactive alerts
- Maintain cabinet security with electronic locks and contact closure sensors
- Optimize strategic and tactical decision making for IT environments by tracking changes in real-time

CONNECT, MONITOR, & MANAGE TODAY

Learn More

1.800.724.8090 | sales@raritan.com | www.raritan.com

Charles Taylor joins the AI battle against fraud by investing in cutting-edge insurtech

Charles Taylor has acquired a majority share of Argentina-based Fraud Keeper.

Charles Taylor, the provider of claims and technology solutions to all parties in the global insurance market, has entered into a partnership with Fraud Keeper (FK), acquiring a majority share of the company.

FK is a cutting-edge SaaS platform based on automation and Artificial Intelligence that helps insurers detect, prevent and manage fraudulent transactions in real time. FK is based in Argentina and has a presence in Spain.

The FK team, which has over 20 years' experience in helping insurers in the fight against fraud, has rapidly built its client base and reputation in Latin America. The partnership with Charles Taylor will enable FK to bring its proven technology to new markets and client situations globally.

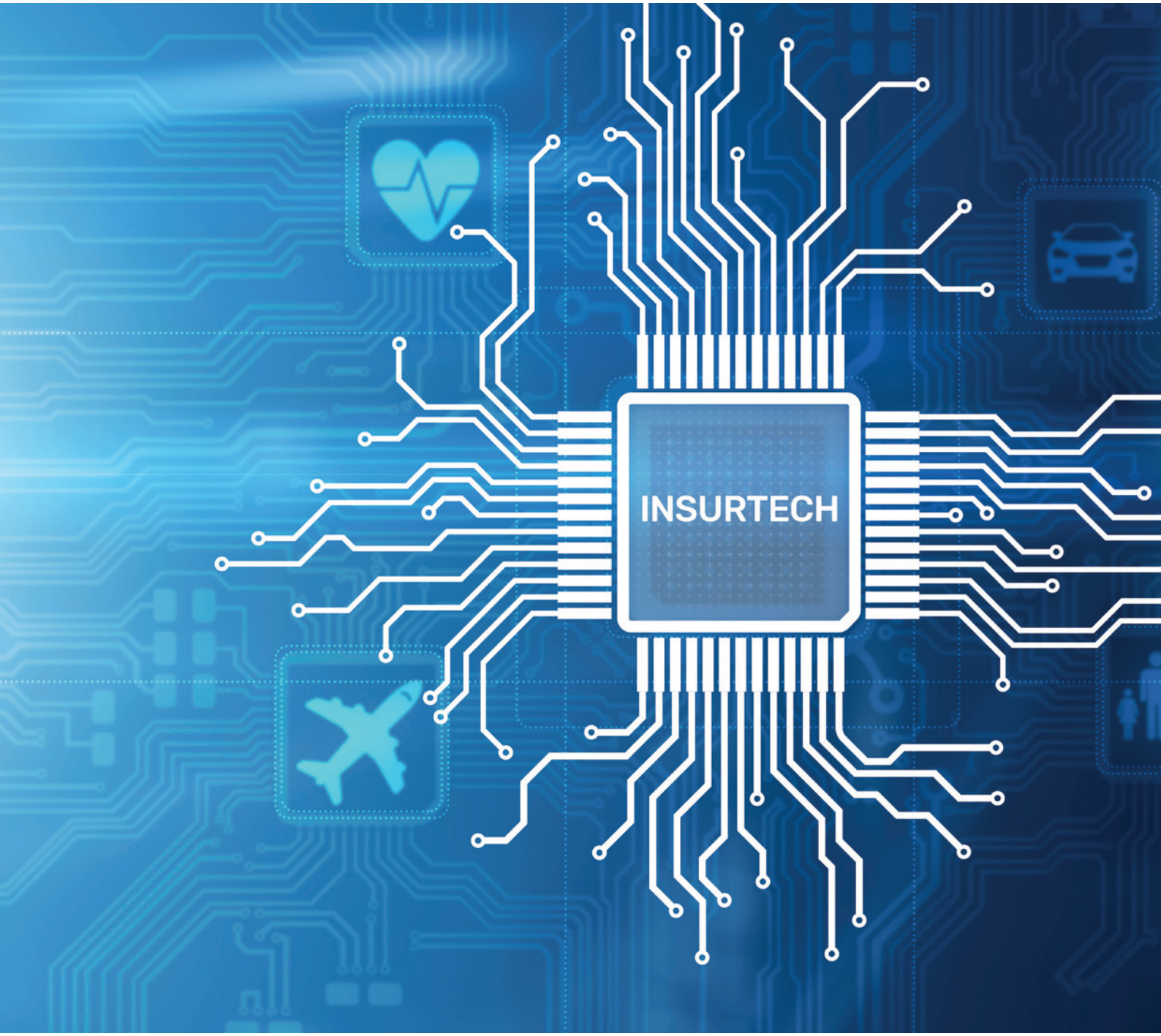
The FK team, which has over 20 years' experience in helping insurers in the fight against fraud, has rapidly built its client base and reputation in Latin America.

Fraudulent claims are a multibillion-dollar industry issue across the global insurance industry and as insurers automate more of the claims lifecycle, the risk of losing money to fraudulent activity is increasing.

FK's automated fraud detection software triages, validates and fast-tracks genuine claims, with automated claims payment functionality to reduce the claims lifecycle. It uses Machine Learning to continually improve fraud detection and links to external data sources to gather additional insights.

The technology can also support smart risk selection and churn prediction with new customers, as well as providing insights to insurers to up-sell and cross-sell relevant products to their existing customer base.

FK will be a valuable addition to Charles Taylor's extensive suite of InsureTech tools and solutions, which already includes Authorities Governance, Distributed Data Management, Claims



Management, Digital Distribution, Document Management, Process Management and Broking Platforms. In addition, FK complements Charles Taylor's global counter fraud strategy, its Specialist Investigation Services investigations division and the acquisition of Contego Investigative Services in January 2022.

Lautaro Mon, Chief Product Officer, Charles Taylor InsureTech, said: "This is a significant step in our strategy to invest in innovation that helps our insurer clients compete in today's fast-moving market.

"The Fraud Keeper technology, combined with our own market-leading suite of products, will be a game-changer for insurers in the fight against fraud. We believe that AI will play a key role in the future of insurance."

Bobby Gracey, Group Head of Fraud, Charles Taylor, said: "Fraud Keeper's technology will enable us to further enhance Charles Taylor's counter fraud ecosystem and help our clients better manage their claims expenses and loss ratios. When automated fraud detection is utilised in conjunction with Charles Taylor's investigative capabilities, it can provide clients with a complete solution to fraud prevention, detection and investigation."

Daniel Gabas, Chief Executive Officer, Fraud Keeper, said: "We are delighted

to be working with Charles Taylor and this new partnership will enable us to scale the business globally.

“Our proven technology, combined with Charles Taylor’s products and services, will enable us to offer our clients true end-to-end solutions.

“We look forward to leveraging Charles Taylor’s technology and expertise in the insurance sector to create a world-class proposition for clients.” ◆

Negligent insiders are the root cause of 56% of cyberattack incidents, while credential thefts have almost doubled and are the costliest to remediate, at an average of over US$800,000 per incident. Proofpoint has released brand-new research showing that businesses globally are losing around £11.4 million (US$15.4 million) every single year because of insider cyberthreats.

Study reveals insider threats cost organisations US$15.4 million annually, up 34% from 2020

Proofpoint, a leading cybersecurity and compliance company, has released its *2022 Cost of Insider Threats Global Report* to identify the costs and trends associated with negligent, compromised and malicious insiders. Notably, on average, impacted organisations spent US$15.4 million annually on overall insider threat remediation and took 85 days to contain each incident.

The report, independently conducted by Ponemon Institute, is issued every two years and is now in its fourth edition. It surveyed over 1,000 IT and IT security practitioners across North America, Europe, Middle East, Africa and Asia-Pacific. Each organisation included in the study experienced one or more material events caused by an insider. The report reveals that over the last two years,

Ryan Kalember, Executive Vice President of Cybersecurity Strategy at Proofpoint

the frequency and costs associated with insider threats have increased dramatically across all three insider threat categories, including: careless or negligent employees/contractors; criminal or malicious insiders; and cybercriminal credential theft.

"Months of sustained remote and hybrid working leading up to 'The Great Resignation' has resulted in an increased risk around insider threat incidents, as people leave organisations and take data with them," said Ryan Kalember, Executive Vice President of Cybersecurity Strategy at Proofpoint. "In addition, organisational insiders, including employees, contractors and third-party vendors, are an attractive attack vector for cybercriminals due to their far-reaching access to critical systems, data and infrastructure. With people now the new perimeter, we recommend layered defences, including a dedicated insider threat management solution and strong security awareness training, to provide the best protection against these types of risks."

With people now the new perimeter, we recommend layered defences, including a dedicated insider threat management solution and strong security awareness training.

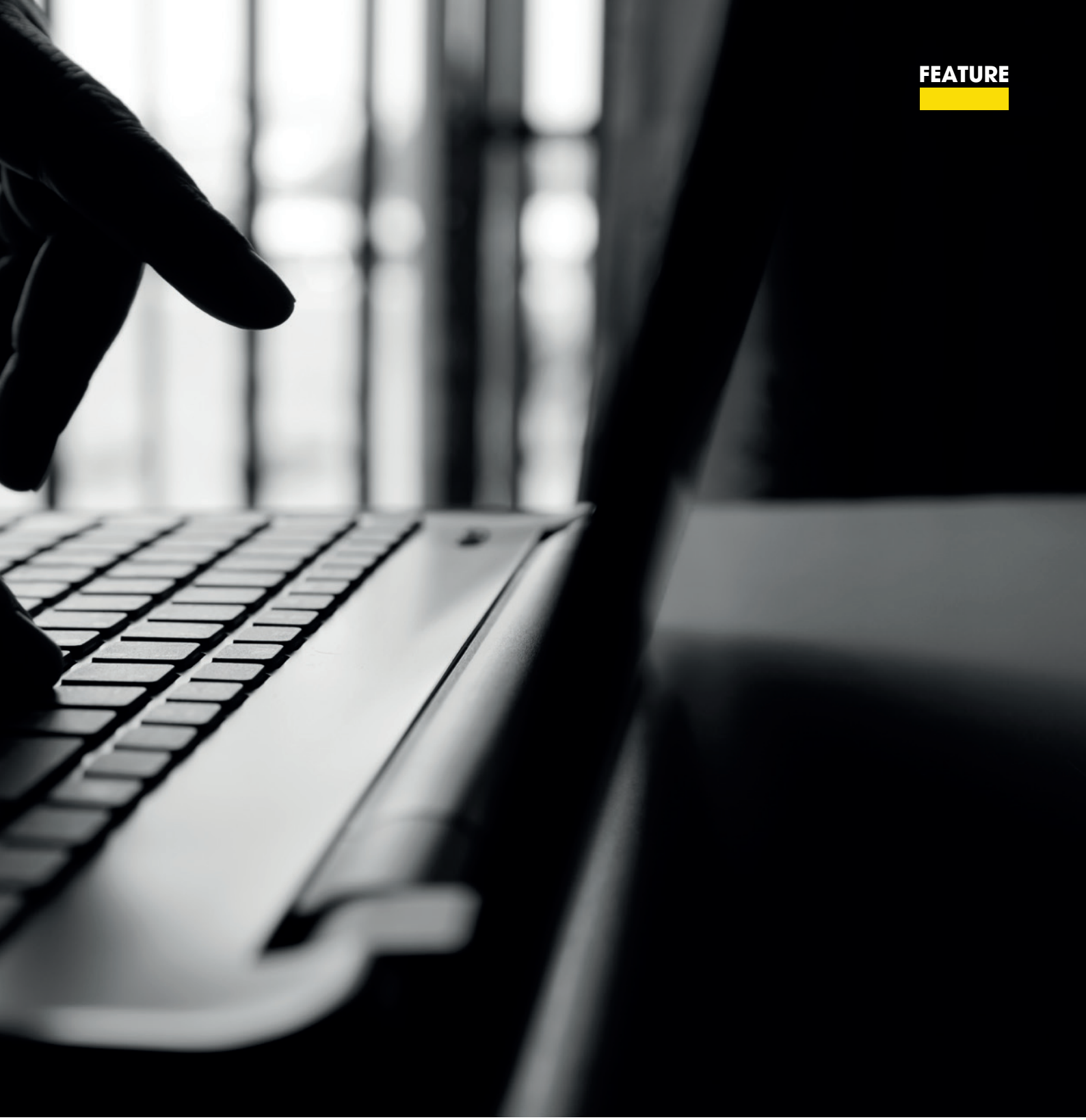
Key findings of this year's *2022 Cost of Insider Threats Global Report* include:

- **Organisations impacted by insider threats spent an average of US$15.4 million annually –** that's up 34% from US$11.45 million in 2020.
- **The overall number of incidents has increased by a staggering 44% in just two years.** The frequency of incidents per company has also gone up, with 67% of companies experiencing between 21 and more than 40 incidents per year, up from 60% in 2020.
- **The negligent insider is the root cause of most incidents.** A high number (56%) of reported insider threat incidents were the result of a careless employee or contractor, costing on average US$484,931 per incident. This could be the result of a variety of factors, including not ensuring their devices are secured, not following the company's

security policy, or forgetting to patch and upgrade.

- **Malicious or criminal insiders were behind one in four incidents (26%) at an average cost per incident of US$648,062.** Malicious insiders are employees or authorised individuals who use their data access for harmful, unethical, or illegal activities. Malicious insiders are harder to detect than external attackers or hackers because employees are increasingly granted access to more information to enhance productivity in today's work-from-anywhere workforce.
- **Credential theft incidents have almost doubled since the last study.** At an average of US$804,997 per incident, credential theft is the costliest to remediate. The intent of the credential thief is to steal users' credentials that will grant them access to critical data and information. A total of an average 1,247 incidents (or 18%) involved cybercriminals stealing credentials.
- **The time to contain an insider incident increased from the last study.** It takes an average of nearly three months (85 days) to contain an insider incident, up from 77 days in the previous study. Incidents that took more than 90 days to contain cost organisations US$17.19 million on an annualised basis, while incidents that lasted less than 30 days cost an average of US$11.23 million.
- **Financial services and professional services have the highest average activity costs.** The average activity cost for financial services is US$21.25 million and professional services is US$18.65 million. Service organisations represent a wide range of companies including accounting, consultancy and professional service firms.
- **Organisational size affects the cost per incident.** The cost of incidents varies according to organisational size. Large organisations with a headcount of more than 75,000 spent an average of US$22.68 million over the past year to resolve insider-related incidents. To deal with the consequences of an insider incident, smaller-sized organisations with a headcount below 500 spent an average of US$8.13 million.
- **North American companies are spending more than the average cost on activities that deal with insider threats.** The total average cost of activities to resolve insider threats over a 12-month period is US$15.4 million. Companies in North America experienced the highest total cost at US$17.53 million.

> North American companies are spending more than the average cost on activities that deal with insider threats.



European companies had the next highest cost at US$15.44 million.

Five signs that your organisation is at risk:

- Employees are not trained to fully understand and apply laws, mandates, or regulatory requirements related to their work and that affect the organisation's security.
- Employees are unaware of the steps they should take to ensure that the devices they use – both company-issued and BYOD – are secured at all times.
- Employees are sending highly confidential data to an unsecured location in the cloud, exposing the organisation to risk.
- Employees break your organisation's security policies to simplify tasks.
- Employees expose your organisation to risk if they do not keep devices and services patched and upgraded to the latest versions.

Dr Larry Ponemon, Chairman and Founder of the Ponemon Institute, said: "Insider threats continue to climb, both in frequency and remediation cost. That said, we are seeing the risk of malicious insider threats increase – with more users accessing business data from outside the confines of the office. This can blur the security team's ability to identify and differentiate between well-meaning employees and malicious insiders trying to siphon sensitive business data." ◆

CYBERARK®

STOP RANSOMWARE IN ITS TRACKS

Only CyberArk provides the most complete and extensible Identity Security Platform to prevent Ransomware attacks.

CYBERARK.COM/RANSOMWARE

EXPERT OPINION

The future CISO is a Chief Trust Officer, according to expert

The convergence of network and security means CISOs are now firmly in the spotlight, becoming the new Chief Trust Officer for their organisations. Tris Morgan, Director of Global Advisory, BT, shares his views on why a Chief Trust Officer is key to driving organisational change across the business.

Tris Morgan, Director of Global Advisory, BT

Right now, many businesses are at different stages of their Digital Transformation journey but, ultimately, one of their main goals remains the same – to have a flexible and secure infrastructure that will support the growth and transformation of the business.

And while historically, network and IT security have always existed as silos, many organisations are now adopting new technologies from Edge to cloud, which are bringing the convergence of network and security closer than ever before.

CISOs are therefore having to cement their leadership and are planting their feet firmly in the role of Chief Trust Officer – driving organisational change to ensure security is always at the heart of the business strategy.

This is increasingly important as security is now a key differentiator for consumers who increasingly look for partners and solutions that instil confidence.

Traditional models are changing

The rapid shift to working from anywhere and acceleration in digital business initiatives brought on by new working models, has shaken traditional business strategies and caused many organisations to review their approach for the better and drive positive change.

But, while we're seeing network and security departments working more closely together, more collaboration is still needed as some advances are still only seen through the lens of the network. In our experience of delivering network and security services, it quickly became clear that although some products start life in our networking division, they need security built in.

For example, many companies still see SD-WAN purely as an opportunity to reduce network costs, and while

> Organisations need to start making sure security is inherent in every business-related decision.

their network teams are usually aware it will increase their organisation's attack surface, what's not taken into consideration is how much visibility and control is lost for the security department.

This is where some traditional structures still remain, which hold back progress. Coupled with organisational silos, skills gaps and existing investments – which will need to be readdressed to help network and security converge even further. Organisations need to start making sure security is inherent in every business-related decision.

> CISOs need to take charge over the trust of both the physical and digital world and expanding their responsibilities across the entire business.

Converging the physical and digital world

It's now even more important to look at physical and cybersecurity in parallel as more devices are being introduced into the operational side of an organisation and connected to the network, creating a larger attack surface to secure. The CISO is no longer just being confined to the digital world, with their role evolving to take on a string of new devices, like control access systems, automated vehicles and even drones, all vulnerable to outside interference and attack.

They have to look at the events from the physical and cyber world together, so that even activity such as internal door alarms alerting against intruders or monitoring door access to restricted areas are seen alongside activity on the network. CISOs need to take charge over the trust of both the physical and digital world and expanding their responsibilities across the entire business.

CISOs are increasingly in the spotlight

As the CISO's role changes, they're taking on a newfound importance in their organisation and becoming the face of trust – driving strategies forward and enabling the business. So, they'll need to make sure the organisation is sufficiently protected from every angle and customer data is always

secure in order to instil the necessary confidence and trust that ensures long-term success and custom. Last year 58% of executives said improving data and network security had become even more important for their organisation.

Plus, there's an opportunity to do more, as 66% also said there needed to be an increased budget for security, increasing the focus on the CISO even more.

Even though expectations are higher than ever, it's providing the CISO with an exciting opportunity to drive change, as we're now seeing many companies making sure security is increasingly at the heart of their Digital Transformation and cloud adoption programmes.

Even though expectations are higher than ever, it's providing the CISO with an exciting opportunity to drive change.

So, how will the role of the CISO evolve?

Introducing the new Chief Trust Officer

The CISO is becoming the face of trust for their organisation, stepping into a newly evolved role as the Chief Trust Officer and taking charge of their organisation's compliance, governance, data privacy and company-wide cyber risk management. ◆

TELEFÓNICA RAMPS UP SECURITY CAPABILITIES FOR SEAMLESS OPERATIONS

The telecommunications industry is one of the most targeted for cyberattacks and telco providers must therefore be on top of their game when it comes to security. Telefónica, one of the world's leading telco companies, has developed innovative solutions – reliant upon 5G technology – to better manage security maintenance tasks and ensure the company can continue operating with a robust cybersecurity culture.

Telefónica Ingeniería de Seguridad (TIS), the Telefónica Group company pioneer in integral technological security, has designed – together with its technological partner Unmanned Life – an innovative solution for managing autonomous drone fleets from a single centralised platform to carry out security, surveillance, event verification and critical infrastructure maintenance tasks.

The solution allows programming an autonomous flight zone in which several aircraft are able to identify events through analytics integrated into the platform with Artificial Intelligence, such as the detection of unauthorised persons at the site and send the images in real time thanks to 5G connectivity, for their corresponding analysis. All of this while complying with all aeronautical legal requirements for drone flight and privacy.

The solution has the capacity to integrate, on the one hand, the event verification function so that drones come to inspect the site in the event of any alarm and, on the other hand, the capacity to detect, identify and neutralise drones. In this way, the solution can detect aircraft at a distance of up to 10km and neutralise them when they are identified as a threat at a distance of approximately 1.5km.

Telefónica Ingeniería de Seguridad's solution is designed especially for companies that lack specialised personnel in these surveillance and security functions or for those that want to assign their human teams to perform other tasks of greater added value in order to gain competitiveness and be more agile in the analysis of the information collected and in decision-making. Its implementation also generates significant time and cost efficiencies of up to 35%, as drones do not require piloting.

The Unmmaned Life platform, which is hardware agnostic, can work with any type of drone. Telefónica Ingeniería de Seguridad carries out technological consultancy for the customisation of drones that best fit the needs of customers, taking into account sensorisation, autonomy, operation, environment, payloads and any parameter that may be involved in the operation.

To demonstrate the benefits and capabilities of the solution, a pilot test has been deployed at the headquarters of Distrito Telefónica in Madrid. In this demonstration, carried out in a highly complex environment from the point of view of regulation due to its proximity to airports and heliports, drones used have a size of 1.20m as well as advanced security systems so that if any unforeseen event arises, such as loss of connectivity or inhibition of communications, they can land in a controlled manner. The drones also have an autonomy of 45 minutes and after this time the aircraft will automatically go to a nearby charging station to fully recharge in about 30 minutes.

This security solution is a pioneer at national level and with Distrito Telefónica being the first corporate headquarters at national level to deploy it, obtaining all the relevant authorisations from the AESA (Spanish Aviation Safety Agency) to carry it out.

"We are very proud to continue helping companies to face the future with greater security and provide solutions for the protection of its assets, infrastructure and employees thanks to the capabilities of technology. With this solution, we not only work with companies as a technology partner, but it also allows us to acquire a consulting role for everything related to the management of drone flights and compliance with regulatory requirements in areas as important as privacy," said Fabián Blanco, Chairman and CEO of Telefónica Ingeniería de Seguridad.

"This is a great first step and a concrete result of our partnership with Telefónica," said Jorge Muñoz, Vice President of Business and Marketing at Unmanned Life. "This innovative product is unique in its style, will set a benchmark in the market and will allow us to demonstrate that it is a secure technology that delivers concrete benefits to users. Together we are building an autonomous future that will improve security and inspections in an optimal, safe and environmentally sustainable way."

Telefónica Tech has also used drones to develop a predictive maintenance solution for electricity grids, with the aim of ensuring their reliability and guaranteeing their proper functioning. Its implementation will increase the safety of companies, improve the quality of the process and optimise costs compared to traditional methods.

The drone used for the inspection of medium and high voltage networks (VTOL, which combine fixed wing with propellers and whose take-offs and landings are performed vertically) has an optical camera, a thermal camera, a LiDAR (remote sensing using laser light) and a gas sensor. The aircraft weighs only 5.5kg, reaches a maximum speed of 100km/h and has a range of up to five hours.

> Telefónica Ingeniería de Seguridad's solution is designed especially for companies that lack specialised personnel in these surveillance and security functions or for those that want to assign their human teams to perform other tasks of greater added value.

The information captured by the sensors is transmitted via 5G for processing with pre-trained Artificial Intelligence algorithms, which combine this data with historical and other external sources to assess which elements require maintenance. If anomalies are detected, the system is able to generate early alerts that indicate the need for more detailed analysis or to establish a new flight for more specific captures.

The solution also has a flight management platform where the drone's functions and movements are controlled, flight missions are planned, annotations are made on the map based on the data collected by the aircraft and video with telemetry information is collected.

"We are very proud to continue innovating and accompanying companies

in their digital development," said Andrés Escribano, Director of New Business and Industry 4.0 at Telefónica Tech.

"The application of drones in the business world presents numerous sectorial use cases that will be expanded and perfected with the massive deployment of 5G. The incorporation of drones in maintenance tasks will allow companies to increase their occupational safety and anticipate possible failures or incidents that without this predictive analysis could end in service outages with their corresponding social and economic impact."

Main benefits

Predictive maintenance of electrical networks with drones has the ability to detect corrosion of insulators and check the temperature of the network in order to identify excessive hot spots that could cause a future failure.

The mapping mapped by the drone flight allows the company to establish safety corridors to prevent fires and trees falling on the towers. In addition, the solution is designed to be able to identify SF6 leaks (a non-toxic gas used in high-voltage electrical equipment) that have a high environmental impact, as well as bird nests and weeds on the towers or cables that could cause power outages.

Telefónica Tech's solution has a direct impact on the prevention of occupational hazards by preventing workers from working at heights or near voltage and improves the quality of work by providing high-precision images that can be processed in a safe environment. It also optimises operational costs and improves operations by avoiding the use of helicopters for these functions, avoiding the need for operators to travel to the area for routine tasks and allowing post-processing from the office. ◆

> Together we are building an autonomous future that will improve security and inspections in an optimal, safe and environmentally sustainable way.

The shift to remote working has highlighted a need for organisations to adapt to an identity-centric approach to their cybersecurity and governance strategies. Craig Ramsay, Senior Solution Consultant, Omada, discusses the management of identities and their associated risk and how business leaders can strengthen their security strategies for the year ahead.

Three identity management trends to consider in 2022

Craig Ramsay, Senior Solution Consultant, Omada

Employers and their workers have adapted to remote and hybrid work and these changes are likely here to stay. Cloud migration has been a major factor in this transition, with some companies merely accelerating their Digital Transformation timelines and others quickly creating digital strategies ad hoc.

Now that the world has had almost two years to adapt, organisations have been able to see what does and doesn't work for both them and their identities. Continuous revaluation of remote and hybrid working strategies are key to maximising productivity and, just as importantly, ensuring it is done securely.

As identities continue to access more and more resources remotely, organisations are faced with increasingly complex security considerations. In fact, attackers pivoted from targeting corporate networks to home networks early in the pandemic because they knew the latter are typically much less secure, as organisations rushed to keep productivity high, security was an afterthought in some cases. In addition, the attack surface proliferated wildly with thousands of new endpoints to potentially exploit as a beachhead into the corporate network.

Thus, this shift to remote and hybrid working has reinforced the idea that identity is central in a strong cybersecurity strategy. The traditional IT security perimeter no longer exists, with many applications and services now hosted in the cloud being accessed by a variety of identities in the office, at home, on the road, or a combination of all of these.

To make sure all identities, including third parties and technical identities, have appropriate and secure access to these new cloud-based and legacy on-premise applications, organisations need to transform the way they deploy and manage their identity governance and identity management initiatives. Combine this with the emergence of Zero Trust and it really has confirmed identity as the ultimate control plane.

With that in mind, let's explore what 2022 will bring in relation to the management of identities and their associated risk.

Ongoing cloud adoption

2022 will see ongoing adoption of SaaS solutions and cloud services. In a survey by Enterprise Strategy Group, respondents reported that 52% of business-critical apps are now cloud-based rather than on-premise – and that number is only growing. Organisations are now able to switch vendors and to scale up services they have been using more easily than ever before. This subsequently increases the threat surface within organisations when it comes to managing identity related risk.

Consequently, organisations need to securely scale with demand and manage their identities across an ever-growing number of applications and services. To meet this need, identity governance solutions must be able to provide a cloud-native foundation of versatile configurability.

> This shift to remote and hybrid working has reinforced the idea that identity is central in a strong cybersecurity strategy.

Greater autonomy in IAM

The year will also bring increased autonomy in identity governance processes. At present, these processes still involve a combination of manual and semi-autonomous activities, meaning that there can be considerable overhead for administrators and end-users. This manual effort combined with the continued shortage of IT and security professionals is not sustainable.

For some time and to varying degrees of complexity, automation has played a role in Identity Lifecycle Management and access provisioning. Automated governance around user access requests, reviews and violation management is less prominent, but recent innovations have seen drastic improvements in prescriptive analytics providing decision support for end-users, reviewers and approvers.

It's true that for the most critical applications and sensitive data, there will always be a need for some level of human decision-making or approval. However, as we see an increase in the amount of useful data held on identities and their access automation of approval, review and violation detection and remediation will also increase to complement the human side of governance.

Intelligent unification

A third new trend I see emerging in 2022 and beyond is the emergence of unified governance platforms. Now, more than ever, organisations have a plethora of solutions at their disposal. This can lead to siloed information and a disparate approach to security where some solutions focus on niche use cases.

Maximising the capabilities and information available and integrating them to provide a unified and holistic view of identities, their access, the contexts, or reasons why they have, and how they use their access will be crucial in reducing identity related risk.

Breaking down these siloes and sharing information across these boundaries will provide assurance that your identities are truly secure and greater adaptability to tackle new identity challenges as they arise.

In addition to this, such platforms will further the autonomy in IGA processes through this meaningful convergence of technology and identity disciplines. This will significantly reduce the manual effort when implementing, managing and interacting with identity governance processes.

Towards an identity-centric approach

The *2021 IBM Cost of a Data Breach* report found that the average total cost of a data breach increased by 10% from the previous year to US$4.24 million – the highest cost ever recorded.

It is now more difficult to both protect against breaches and more costly to deal with their aftermath. Identity governance has never been more important. But now that the traditional corporate perimeter no longer exists, how do you adapt to an identity-centric approach to your cybersecurity and governance strategy?

The last two years have ushered in a sea of change regarding how organisations manage identities and their access. Hybrid working and cloud-based applications and services create greater opportunities for anytime, anywhere productivity but also increase the complexity of managing identity-related risk.

The right solution coupled with the right strategy will enable you to realise the benefits of these opportunities without sacrificing security or efficiency.

The continued adoption of cloud-based services and applications will dovetail with the advent of unified identity governance platforms and an emphasis on greater autonomy. With the automation capabilities available today, there's no need to saddle administrators and end-users with the burden of unnecessary manual effort in managing identity related risk.

What's more, it's now possible to have a holistic view of identity that better serves the diverse needs of all hybrid work scenarios. Take time to reflect upon the three trends noted above and determine whether changes need to be made to your identity strategy for the year ahead. ◆

MISSION ACCOMPLISHED: ASKLEPIOS PROTECTS ITS PATIENTS WITH VMWARE

Armed with an ultramodern IT infrastructure built on the firm digital foundation of VMware, one of Germany's leading hospital operators is ideally placed to meet the needs of today and tomorrow whilst bolstering its reputation as a trusted, security-conscious healthcare group. Here, Daniel Maier-Johnson, CISO at Asklepios, tells us how cybersecurity solutions empower him and his IT team not only to ward off cyberattacks, but also to analyse activities on the devices, adjust preventive measures in response to new threats and automate previously manual workflows throughout the entire security infrastructure.


Daniel Maier-Johnson, CISO at Asklepios

The Asklepios Group is one of Germany's largest private hospitals. 'The highest standards of medical treatment and a commitment to continuous improvement above and beyond what is required by law' have established the Hamburg-based hospital group as a benchmark in the German healthcare sector. Asklepios has advanced to the forefront of digitalisation, tearing down system silos, streamlining data sharing and developing a robust security architecture for its countless devices. Today, VMware Horizon and Workspace ONE are the beating heart of the healthcare provider's IT landscape. VMware Carbon Black Cloud Endpoint Advanced, a cloud-based security solution, combines with VMware Carbon Black App Control for critical infrastructure protection to maximise security across the group's virtualised data centre. Thus, 2.6 million patients served every year at Asklepios hospitals benefit from excellent standards of treatment and medical research, and also from personalised processes and faster diagnoses.

Laying the technological foundation for innovation

People are and always have been at the centre of everything Asklepios does. Even when it started as a small, family-run company back in 1985, Dr Bernard gr. Broermann had a crystal-clear focus on one thing: patients' well-being. Nearly 35 years on, the Asklepios Group has an impressive 67,000 people on its payroll at 170 medical facilities in 14 German states. It serves the needs of 2.6 million patients a year. With high investments in cutting-edge medicine and digitalisation as well as the acquisition of MediClin AG and RHÖN-KLINIKUM AG, Asklepios is playing a key role in driving innovation in the healthcare sector. Since Medilys Laborgesellschaft GmbH acquired a majority stake in the company, Asklepios has also had one of Europe's largest medical laboratories at its disposal. The hospital's ambition is to lead the way in the digitalisation of healthcare in Germany, to further improve the quality of patient care and to shape the medicine of tomorrow.

Digitalisation in the service of humanity

Personalised and patient-centric processes, fast diagnosis, efficient treatment, optimal outcomes and a positive patient experience: The Hippocratic Oath has long ceased to

> VMware Horizon and Workspace ONE are the beating heart of the healthcare provider's IT landscape.

be the only factor in making patients well again. Digital Transformation is now ensuring that many mutually interdependent hospital routines run more efficiently, reliably and closer to the patient. Insular systems that have grown over time are isolated, and complex processes are a common reason why modern digital technology is badly needed in this industry. But there is also a need for strict security. Today – and above all tomorrow – the fast, reliable and seamless sharing of information and the straightforward deployment of systems and devices will be decisive for Asklepios' medical processes. At the same time, the technological foundation must be laid for continuous standardisation, interoperability, security and innovation.

"We obviously have a very strong focus on cybersecurity," said Daniel Maier-Johnson, Chief Information Security Officer (CISO) at Asklepios.

In the area of privacy and data protection, the healthcare sector cannot afford half-measures. These sort of attacks are a threat to patients' identity and they can impede hospital operations and place the health and well-being of patients at risk. The hospital operator therefore took swift action when a risk assessment performed by Maier-Johnson revealed moderate potential for improvement. To ensure patients and their data will not be exposed to threats from cyberattacks, top priority was given to modernising security processes. The new concept had to measure up to the requirements of Germany's critical infrastructure laws, but they also had to function with as few staff as possible. Beyond warding off threats, the new solution had to be intelligent enough to learn constantly.

'VMware fits in with our ecosystem'

The Asklepios group set out to find a flexible, agile security platform into which new systems and endpoints could be integrated quickly and easily. "We launched an evaluation process, but the only really viable option for our enterprise requirements and our many thousand endpoints was VMware," said Maier-Johnson. "That is especially true when you need to combine extensive standardisation and automation with maximised availability."

It helped that the hospital group had already been working with proven virtualisation solutions for 16,000 workspaces based on VMware Horizon and Workspace ONE. VMware vSphere was in place as part of a long-standing partnership with the digital solution provider. The cloud-based security

> To ensure patients and their data will not be exposed to threats from cyberattacks, top priority was given to modernising security processes.

solution, Carbon Black Cloud Endpoint Advanced, and Carbon Black App Control now maximise security across the hospital operator's virtualised data centre. Carbon Black Cloud Endpoint Advanced is a next-generation antivirus solution that also provides endpoint recognition and response capabilities based on behavioural patterns. It includes Carbon Black Cloud Audit & Remediation, a real-time audit and correction solution that gives Asklepios' security teams fast, easy access to unified data and enables them to adjust the system status of endpoints and containers.

Improvements for staff and patients alike

Thanks to VMware Horizon and VMware Workspace ONE, Asklepios' staff can work from anywhere with access to a secure, high-availability platform. Nursing staff can, for example, use mobile devices to tap into everything they need to know about patients anywhere in the building.

"We see VMware as an investment in improving the way our people work, from senior doctors to nurses," said Henning Schneider. "We are harnessing the opportunities afforded by digitalisation to continually optimise the quality of healthcare, but also to ease the workload on our colleagues. By 2024, our plan is to be a fully digital healthcare group."

Maier-Johnson stresses that there were no missteps when implementing the security solutions – both Carbon Black Cloud Endpoint Advanced and Carbon Black App Control were up and running smoothly in under two months. Carbon Black Cloud empowers the CISO and his IT team not only to ward cyberattacks, but also to analyse activities on the devices, adjust preventive measures in response to new threats and automate previously manual workflows throughout the entire security infrastructure.

The confidentiality of patient data thus remains securely protected. The Carbon Black App Control is able to control critical servers and systems to prevent undesirable modifications and guarantees consistent compliance with all relevant legal specifications.

As a result, it is easy for the staff of Asklepios to work from anywhere – and to do so using virtual desktops that are more securely protected.

Even the unprecedented circumstances relating to the Coronavirus have created no problems.

"Thanks to VMware, we were able to respond flexibly to the pandemic," said Maier-Johnson. "We were immediately able to work securely from home."

Former IT silos are also not an issue, given that data sharing now meets the highest standards. It is much safer and more convenient to use patient portals, access the wireless LAN in the cafeteria or book appointments online.

"By guarding sensitive patient data against cyberattacks and data breaches, we are bolstering our reputation as a trusted, security-conscious healthcare group," Maier-Johnson said.

Thanks to VMware, the hospital operator can do more than merely keep up with constant changes in the industry, it can also respond quickly and flexibly to medical advances and changing political conditions. As Maier-Johnson sees it, these cutting-edge technologies make Asklepios more attractive to new employees and is an integral aspect of their success. Ultimately, the 2 million+ patients served every year at the Asklepios hospitals benefit from excellent standards of treatment and medical research, and also from personalised processes and faster diagnoses.

AI and robotics for medical innovation

Building on this experience, the Asklepios Group is keen to leverage its IT to also tap into new lines of business. Going forward, there are plans for additional IT services for internal use and for a new self-service platform for apps. Preparations are underway to use VMware SD-WAN by VeloCloud to protect medical devices, too. The aim is for largely insular medical equipment to be incorporated in the Asklepios network with all key security functions. "Digitalisation will help new digital services and offerings to emerge," said Maier-Johnson. "For the future, we are thinking about the greater use of AI, automation and robotics innovations for both patients and staff. As such, we are driving advances in medical care." ◆

There's never been a better time to move forward.

Delivering vaccines to millions of people in months, not years.

Reducing customer service response times from 2 days to 2 seconds.

Bringing groceries to your doorstep in under 30 minutes.

The right data is a springboard for leaders who want to bring their vision for their company to life faster, sooner.

Cloudera's enterprise data cloud platform helps our customers move their teams and their companies forward to thrive.

CLOUDERA

Data That Moves You

cloudera.com/datamovesyou
#datamovesyou

Menlo Security finds cloud migration and remote work gives rise to new era of malware

Menlo Security, a leader in cloud security, has announced it has identified a surge in cyberthreats, termed Highly Evasive Adaptive Threats (HEAT), that bypass traditional security defences. HEAT attacks are a class of cyberthreats targeting web browsers as the attack vector and employ techniques to evade detection by multiple layers in current security stacks, including firewalls, secure web gateways, sandbox analysis, URL reputation and phishing detection. HEAT attacks are used to deliver malware or to compromise credentials, which in many cases leads to ransomware attacks.

In an analysis of almost 500,000 malicious domains, the Menlo Security Labs research team discovered that 69% of these websites used HEAT tactics to deliver malware. These attacks allow bad actors to deliver malicious content to the endpoint by adapting to the targeted environment. Since July 2021, Menlo Security has seen a 224% increase in HEAT attacks.

HEAT attacks leverage one or more of the following core techniques that bypass legacy network security defences:

- **Evades both static and dynamic content inspection:** HEAT attacks evade both signature and behavioural analysis engines to deliver malicious payloads to the victim using innovative techniques such as HTML Smuggling. This technique is used by threat actors including Nobelium, the hacking group behind the SolarWinds ransomware attack. In one recent case, dubbed ISOMorph, the Menlo Labs research team observed the campaign using the popular Discord messaging app to host malicious payloads.
- **Evades malicious link analysis:** These threats evade malicious link analysis engines traditionally implemented in the email path where links can be analysed before arriving at the user.
- **Evades offline categorisation and threat detection:** HEAT attacks evade web categorisation by delivering malware from benign websites, either by compromising them or patiently creating new ones. Referred to as Good2Bad websites. Menlo Labs has been tracking an active threat campaign dubbed SolarMarker, which employs SEO poisoning. The campaign started by compromising a large set of low-popularity websites that had been categorised as benign, infecting these websites with malicious content.
- **Evades HTTP traffic inspection:** In a HEAT attack, malicious content such as browser exploits, cryptomining code, phishing kit code and images impersonating known brands' logos is generated by JavaScript in the browser by its rendering engine, making any detection technique useless.

"With the abrupt move to remote working in 2020, every organisation had to pivot to a work from anywhere model and accelerate their migration to cloud-based applications," said Amir Ben-Efraim, Co-founder and CEO of Menlo Security.

"An industry report found that 75% of the working day is spent in a web browser, which has quickly become the primary attack surface for threat actors, ransomware and other attacks.

"The industry has seen an explosion in the number and sophistication of these highly evasive attacks and most businesses are unprepared and lack the resources to prevent them. Cyberthreats are a mainstream problem and a boardroom issue that should be on everyone's agenda." ◆

Run and Transform

Different tracks. Same race.

Micro Focus is the official technical partner of Jaguar Racing. We provide world-class software to support Jaguar's push for more points, podiums, and wins—both on and off the track in the fast-changing environment of the ABB FIA Formula E World Championship.

Learn about our partnership at microfocus.com/jaguarracing

MICRO FOCUS | JAGUAR RACING FORMULA-E TEAM

OFFICIAL PARTNER

Pure Storage enables organisations to close the ransomware security gap

Pure Storage, an IT pioneer that delivers Storage-as-a-Service in a multi-cloud world, has addressed the state of ransomware security among modern businesses, highlighting the importance of backup and recovery to build a comprehensive data protection strategy.

Ransomware attacks are becoming increasingly common in today's digital world, presenting a frequent and expensive risk to businesses everywhere. In fact, Cybersecurity Ventures predicts that the global damage caused by ransomware could cost up to US$265 billion by 2031. While organisations have recognised the risks, there's still a gap in understanding where current security measures are and where they should be.

"Faced with the increasing risk of attacks, I was looking to guarantee the protection of our data in terms of backups and against ransomware," said Marc Duong, CISO-CIO, Solidéo (Société de Livraison des Ouvrages Olympiques).

> Pure helps organisations close this security gap, enabling global businesses to safeguard their data against loss, corruption and growing cybersecurity threats.

"I chose to protect them more efficiently by using storage technology rather than server and by taking snapshots very regularly with Pure."

With its data protection portfolio – including Pure SafeMode on FlashArray and FlashBlade, Pure FlashRecover, powered by Cohesity, launched one year ago and Portworx PX-Backup – Pure helps organisations close this security gap, enabling global businesses to safeguard their data against loss, corruption and growing cybersecurity threats.

"Implementing a meaningful data protection strategy, taking a before, during and after approach to planning, is vital to running a successful business today," said Paul Singh Ahuja, CTO, Security, Pure Storage. While having the proper precautions in place to prevent an attack is essential, it's equally as critical that organisations plan for recovery. Pure's solutions are uniquely positioned to help customers rapidly restore data, at scale, to avoid Business Continuity disruptions and negative financial impact."

By leveraging Pure's data protection solutions, global customers can truly secure their data and take advantage of a comprehensive data protection strategy.

"With billions of dollars at stake and their reputations on the line if systems go down, our clients need reliable, secure data services," added Jesse Bonserio, Senior Director of Engineering, Abacus Group. "That's exactly what Pure Storage enables us to deliver, positioning us to build strong client relationships for the long term." ◆

MekongNet and IPification launch one-click mobile authentication with enhanced security in Cambodia

MekongNet, a leading Internet Service Provider and A2P messaging aggregator in Cambodia, has joined forces with IPification, the one-click mobile identity solutions provider, to deliver the next-generation of seamless mobile data authentication services in Cambodia.

> End-users can verify their identity with a single tap based on their mobile ID key which consists of their IP address, phone number and device data.

IPification's collaboration with MekongNet will drive the deployment and adoption rate of this service by enterprises in Cambodia.

IPification is currently the only global provider of mobile IP address-based authentication and identity solutions. End-users can verify their identity with a single tap based on their mobile ID key which consists of their IP address, phone number and device data.

In addition to security, companies also get to streamline the onboarding and user experience for their users.

IPification had partnered with MekongNet earlier in 2021 and MekongNet has since further developed API/SDK enhancements around IPification's solution including account management, deployment and operations support features,

service monitoring and reporting to enhance the offering of the Mobile Data Authentication service to enterprises.

"MekongNet has a huge presence in Cambodia and I am very happy that together we can enable top-notch security in the enterprise landscape in the country," said Stefan Kostic, IPification CEO. "Apart from security, I am looking forward to seeing the effects frictionless mobile authentication and phone verification will have on productivity within these companies." ◆

Armis and Eseye announce availability of solution to secure connected devices on cellular networks

Global connectivity specialist, Eseye, and leading agentless device security platform provider, Armis, have announced the general availability of a joint solution that enables organisations to deploy connected devices anywhere in the world with enterprise-class security and consistent, reliable cellular (4G/LTE/5G) connectivity.

Digital Transformation created a new generation of connected things that extend beyond traditional IT and across virtually every business and industry. For the first time, the volume of these non-traditional assets has surpassed the total number of traditional computers and servers globally. Analysts predict this number will multiply exponentially in the next five years. This new hyperconnected, highly distributed and dynamically changing environment represents digital businesses' new cyberasset landscape. Any loss of connectivity or cyberattacks against these devices can be financially devastating and brand-damaging, causing widespread collateral loss to an organisation's bottom line.

"Most traditional endpoint security products available today require agents which cannot install on the majority of cellular-based IoT and OT devices," said Peter Doggart, Chief Strategy Officer, Armis. "These devices control the temperature of food and medicine storage, update maintenance information on airplanes, or control critical infrastructures like power and water transmission and they are exposed with grave risk of cyberthreats. The footprint of these devices is expected to expand rapidly over the coming years, making the joint solution from Armis and Eseye an ultimate foundation for automation and Digital Transformation."

Many of these new connected devices use 4G/LTE/5G technologies, which increases their range and flexibility while introducing unique challenges for connectivity and security.

Outside of North America, hundreds of Mobile Network Operators (MNOs) operate across geographies with many shared borders, creating a lack of persistent connectivity.

Most carriers prevent devices from roaming after a few weeks, dramatically impacting the ability of cellular-based IoT and other devices to realise their full potential. According to Eseye's 2021 State of IoT Adoption Report, over one-third (35%) of survey respondents cited cellular connectivity as the main challenge to rollouts of large-scale IoT projects.

Eseye's unique Connectivity Management Platform enables devices to switch intelligently to any one of over 700 GSMA-compliant carriers to maximise uptime with near 100% global coverage. The Armis Agentless Device Security Platform provides device discovery, monitoring and behavioural risk assessments to respond automatically to anomalies that put devices at risk. Together, this joint solution ensures organisations can deploy and access virtually any device globally with confidence.

"With Transforma Insights predicting that the number of cellular devices will increase to five billion by 2030, the IoT attack surface is growing exponentially," said Nick Earle, CEO of Eseye. "The emergence of eUICC and eSIM means devices can frequently move between a range of public and private 5G networks, as well as IoT platforms, making IoT assets hard to track and secure." ◆

Atos develops video system for future surveillance aircraft of France's Navy

Atos has announced that it is supporting Dassault Aviation to develop and produce the inflight video system for its 'Falcon Albatros'. The latter is the future maritime surveillance and intervention aircraft of the French Naval Aviation. The 'Albatros' is set to be commissioned in 2025 as part of the AVSIMAR programme led by the French Armament General Directorate (Direction Générale de l'Armement, DGA). The aircraft will leverage the capabilities of the French Navy (Marine nationale), delivering homeland maritime protection and defence.

The AVSIMAR programme provides a response to the challenges of French government action at sea. These include fighting pollution and trafficking, border surveillance and exclusion zones as well as search and rescue at sea. Spearheading the programme, the Albatros is equipped with a next-generation mission system and high-performance sensors. The aircraft features a multifunction radar, multispectral optronic turret, observation windows, a Search and Rescue (SAR) kit release system and dedicated communication systems. Combined, these sensors enable HD video and data streams, producing real-time analysis and fully enhancing tactical situation awareness.

Atos will manage the design and production of the inflight video system, which ensures the compression, distribution and transmission of various data and tactical videos on board while taking into account IT security issues.

As such, Atos will ensure that the system meets strict security requirements by verifying the integrity and authenticity of data software and by providing secure data and video interconnections.

Atos' solution is focused on key foundational issues of Maritime Surveillance Aviation. To this end, the group will successfully consolidate mission-critical, secure and reliable data while supporting the development of military aircraft. The solution guarantees optimal performance in all of the French Naval Aviation's missions and within a secure technology environment.

"We are proud to assist Dassault Aviation in preparing the Falcon Albatros aircraft which will support the French government in its maritime surveillance and intervention missions," said Cyril Dujardin, SVP, Head of Digital Security at Atos. "Through this strategic project, we are strengthening our long-standing relationship with Dassault Aviation with a focus on inflight systems. In doing so, we are also applying our expertise to deploy security mission systems and fibre optic HD videos." ◆

Pangiam and Google Cloud collaborate to transform aviation security

AGS Airports Ltd to trial new Artificial Intelligence-led technology at security sites in Aberdeen, Glasgow and Southampton airports.

Pangiam, in collaboration with Google Cloud, has announced details of Project Dartmouth, an initiative to transform airport security operations by looking for threats concealed within baggage and other shipments at the airport.

Project Dartmouth will utilise Pangiam's technologies alongside Google Cloud's Artificial Intelligence (AI) and Machine Learning (ML) computer vision tools, such as their Vertex AI Platform.

This technology will be tested within the security facilities of AGS Airport Ltd, owners and operators of Aberdeen, Glasgow and Southampton Airports in the UK.

The collaboration means that Pangiam's national security-grade technology and deep experience of managing aviation security threats will, for the first time, be boosted by Google Cloud's industry-leading suite of AI technologies.

Project Dartmouth is intended to make air travel safer by integrating AI into airport baggage security and screening operations. The technology will in the first instance be focused on rapidly identifying potential threats in baggage, providing increased throughput at security checkpoints, addressing critical friction points in air travel as well as supporting security teams. In later phases the technology will scale to help tackle other pressure points in security and wider airport operations.

AI and ML models will be trained to be able to detect prohibited items in real-time as bags pass through airport X-ray scanning equipment.

It will also be used to spot anomalies and unusual patterns which could indicate a new or co-ordinated attempt to breach security, before alerting security staff to examine those items further.

Alexis Long, Chief Strategy Officer for Pangiam, said: "This technology marks a monumental step in bringing automation to aviation security and sets a new precedent for international security standards.

“First and foremost, the technology will deliver a better experience for the traveller, the airport and governments. To help us achieve this, we have selected Google Cloud as our technology vendor of choice – a leader in Artificial Intelligence and cloud technologies."

Mark Palmer, Head of EMEA Public Sector, Google Cloud, added: "We are delighted to collaborate with Pangiam on this ground-breaking initiative to protect AGS's network of passengers and customers. The power of Artificial Intelligence is boundless and we look forward to improving the aviation industry at large."

Chief Operating Officer of AGS Airports Ltd, Mark Johnston, said: "Google Cloud and Pangiam are world leaders in the Artificial Intelligence field and we are pleased to be working in partnership with both organisations on a cutting-edge project that could have a transformative effect on the security of our passengers and colleagues.” ◆

DON'T DELAY ON ZERO TRUST – REVIEWING SECURITY STRATEGIES FOR 2022

With the development and adoption of new technologies, the threatscape has inevitably widened and prioritising a cyber-resilient workforce and Zero Trust model are key to determining an organisation's cybersecurity culture. PJ Kirner, CTO and Co-founder at Illumio, discusses security spending and strategy building, as well as developing a robust Zero Trust approach to cybersecurity.

PJ Kirner, CTO and Co-founder at Illumio

As cyber-risk levels continue to rise, CISOs are under intense pressure to keep the wheels turning while also preparing for inevitable future attacks. Businesses can no longer afford to take their time crafting the perfect long-term security plan before they commit – they need to act proactively now to deal with current threats.

Having a strong and cohesive security foundation is critical for navigating today's cyber landscape and taking a Zero Trust approach has become a non-negotiable for businesses. Skyrocketing ransomware and cyberattacks paired with remote work and Digital Transformation are pushing organisations to build resilience – and fast. Illumio recently commissioned a study with Forrester Consulting to explore how organisations are using Zero Trust strategies to navigate the current landscape and to understand what their security plans are for 2022.

Zero Trust is one of the most effective approaches in enabling organisations to improve their resilience and take a more proactive approach to security. To be clear, according to Forrester Research, 'Zero Trust is not one product or platform; it's a security framework built around the concept of 'never trust, always verify' and 'assuming breach'.

Importantly, the research study also highlighted that micro-segmentation is a critical pillar of any Zero Trust strategy. The study says, 'Micro-segmentation is fine-grained control of application needs, user access and data repositories. Tools help automate, orchestrate, test and implement granular policy across network security controls'. This control is a cornerstone of security leaders' approach to tackling ransomware and other threats in 2022.

Security spending and strategy building

The dynamic nature of the cybersecurity landscape often forces businesses to switch focus at the drop of a hat. Rapid changes can leave organisations bewildered, for example, Illumio's research found that 63% of respondents said their firm was unprepared for the quickened pace of cloud transformation and migration. Consequences of this lack of preparation can include a drop in productivity and create more opportunities for cyberattacks.

This ongoing Digital Transformation continues to impact strategic focus

START SAVING MONEY TODAY WITH IBM GUARDIUM

FORRESTER®

The Total Economic Impact Of IBM Security Verify

Through customer interviews and data aggregation, Forrester concluded that IBM Security Verify has the following three-year financial impact.

"IBM Security Verify is a very comprehensive platform with SSO, MFA, and identity governance suitable for all our constituents including business-to-employee, business-to-business, and business-to-consumer use cases."

Interviewed customer

User benefits over three years: **$10.1M**

Developer benefits over three years: **$269K**

Infrastructure cost avoidance benefits: **$82K**

VOICE OF THE CUSTOMER

"I know the benefits created by Security Verify have exceeded the costs. We are saving money in the areas of infrastructure cost avoidance, IAM administration, and the ability of developers to integrate identity-related functions into applications."

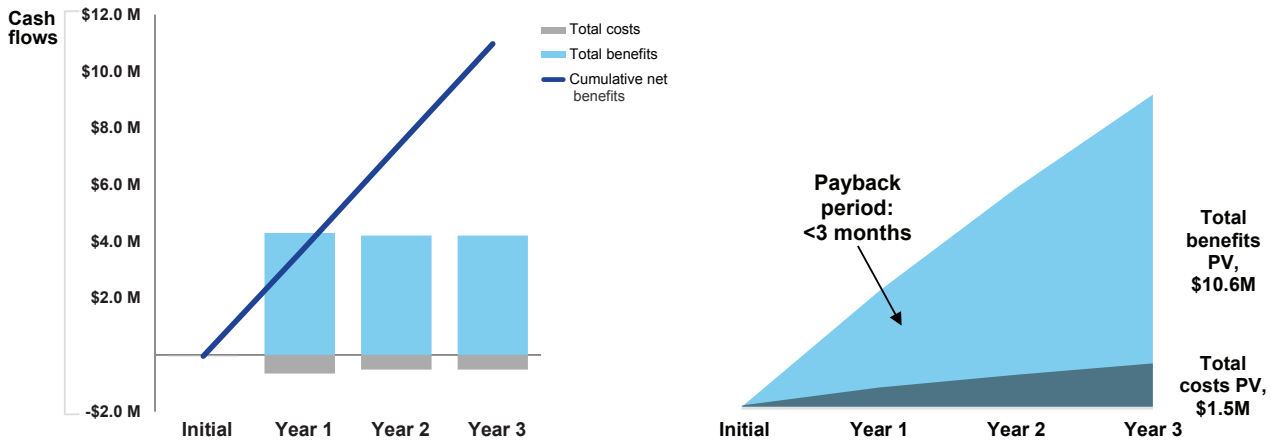
Interviewed customer

FINANCIAL SUMMARY

Three-year risk-adjusted

ROI	NPV	PAYBACK
619%	$9.1M	<6 months

CASH FLOW CHART (RISK-ADJUSTED)



Gold Business Partner

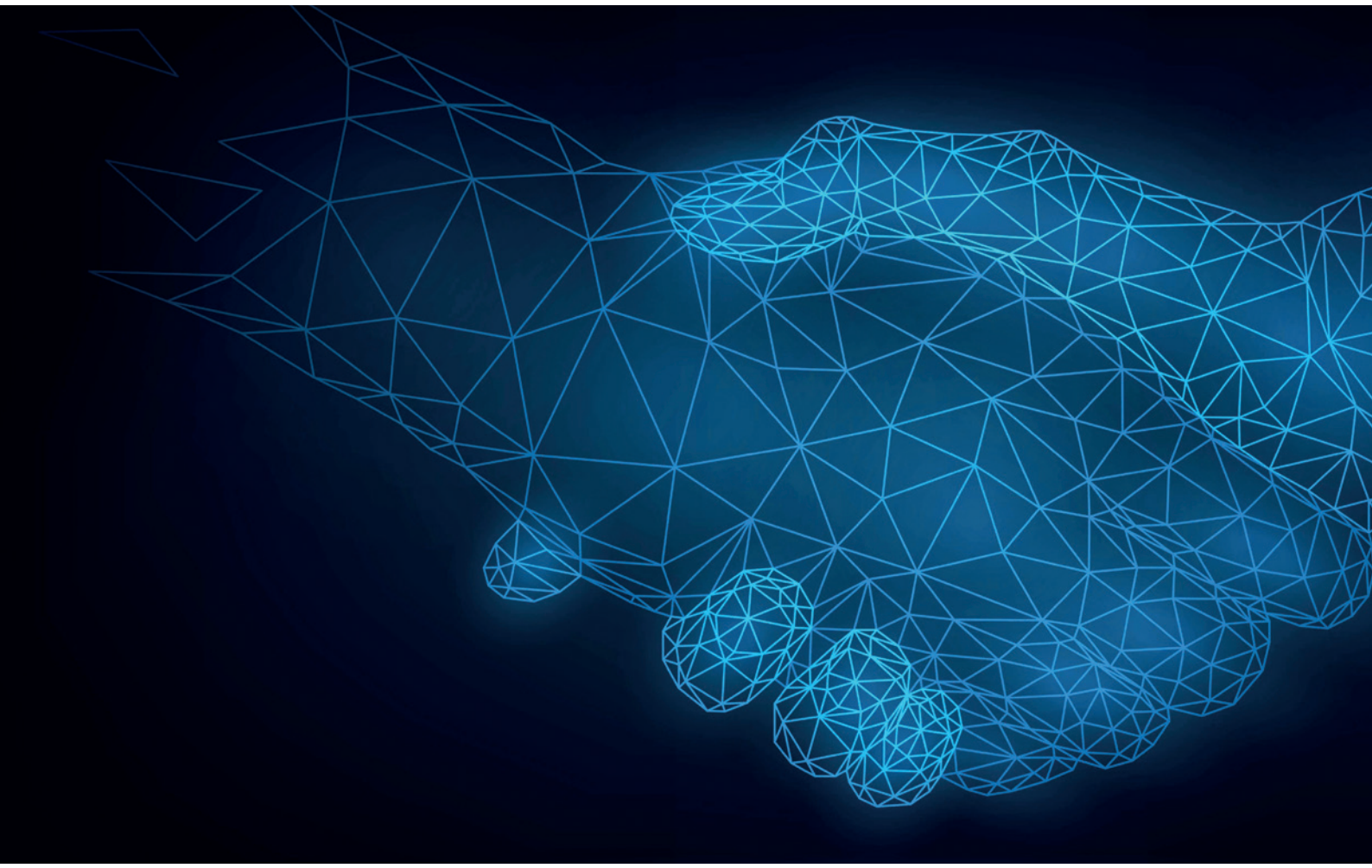
IBM

FIREWARE KNOWLEDGE PROTECTED

Contact Fireware to find out more

43% Improved detection of accurate threats
67% Increased discovery of vulnerabilities & misconfigurations
50% Enhanced data classification

Zsofi Harsanyi - zsofi.harsanyi@fireware.com
http://www.fireware.com



and security spending as firms fight to stay ahead of the curve and anticipate future challenges. For example, 75% of decision-makers switched focus to updating technical reference architectures for cloud security to match rapid cloud migration. In fact, businesses are increasingly prioritising security, as experts forecast the global cybersecurity spending to exceed US$1.75 trillion by 2025.

As part of this prioritisation, more and more businesses are looking to Zero Trust strategies to support cloud migration in order to account for new security gaps and build resilience at scale. However, many enterprises are still in the early stages of implementation, with only 36% having started to deploy their Zero Trust plans. So, while businesses are starting to focus on least privilege security controls, there is still a long way to go in making organisations more resilient to breaches.

> Having a strong and cohesive security foundation is critical for navigating today's cyber landscape and taking a Zero Trust approach has become a non-negotiable for businesses.

And while it's promising to see that two-thirds of businesses will increase their Zero Trust budget, it's important to remember to . . .

Budget incrementally – it doesn't have to be all or nothing

All too often organisations stall or postpone security progress because of financial cost. Of course, security teams need to advocate for their major projects, but it's also crucial to make incremental progress now with the resources you have today.

A good place to start is by gaining an understanding of both the

communications currently happening in your environments, and the connections that could happen. This will illuminate risky areas and help you prioritise where to implement Zero Trust controls.

Then, focus on securing your riskier and business-critical applications and expand as your budget allows. You can make incremental progress on your strategy rather than trying to tackle everything all at once. Concentrate on developing and implementing Zero Trust plans one step at a time to start building resilience today.

Aside from building business resilience, security leaders believe Zero Trust strategies improve their organisations' agility and support their overall Digital Transformation. In fact, around half of respondents said micro-segmentation specifically can help them reduce their attack surface and 68% said micro-segmentation enhances security to support expanded remote, work-from-anywhere models.

The barriers to success

There are two main challenges that can hinder Zero Trust progress: a lack of expertise and stakeholder investment.

The current skills shortage means that security expertise is in short supply and internal teams struggle to find the time they need to act on many of their goals.

Consequently, 62% of decision-makers chose to implement data centre firewalls instead of micro-segmentation. However, this only led to more problems: the firewalls took too long to deploy, were difficult to scale and exceeded the budget.

Additionally, it's true that having strong buy-in from stakeholders can advance Zero Trust implementation, but one of the issues is that these stakeholders often view 'Zero Trust' and 'micro-segmentation' as marketing buzzwords that hold little weight in relation to the larger cybersecurity picture.

However, security professionals understand the resilience, flexibility and scalability Zero Trust and micro-segmentation provide and must translate the value and urgency of these strategies to their stakeholders – the integrity of the organisation relies on it.

While skill and resource challenges are important considerations, they should not get in the way of organisations starting their Zero Trust journey.

Teams can start small and work their way up, gathering new skills and winning over stakeholders as they go.

Finding simple ways to start segmenting

Like the past few years, 2022 demands that enterprises balance business operations and security in order to prosper. Micro-segmentation solutions need to enable organisations to maintain this fine balance.

Segmentation solutions must provide simple and approachable on-ramps. If they require a system overhaul, you're going to get stuck at your starting blocks. If they don't scale, you're going to get early technical detractors.

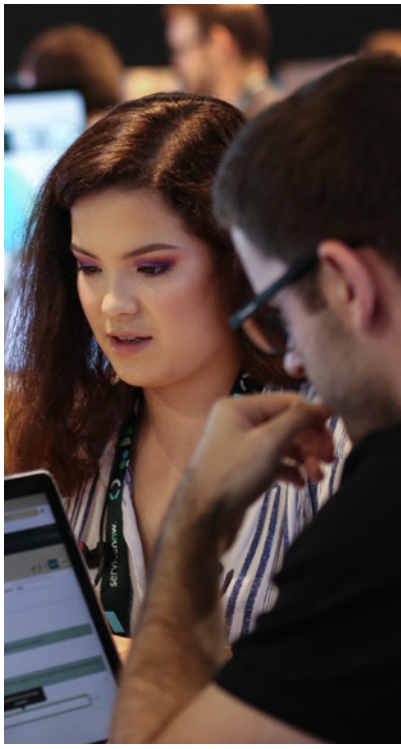
If they don't adapt as your network changes, the friction will cause rejection of the solution. And if you don't have some quick wins to demonstrate to your boss and your board, you never fulfil the strategic goals.

Already, 73% of decision-makers consider Zero Trust and micro-segmentation to be critical technical foundations of their security strategy and we expect this number to continue to grow as understanding of these approaches increases. Security leaders recognise the value of segmenting their networks to isolate a breach by proactively blocking attackers from moving around to access critical data. Understanding its importance, businesses need to start implementing their Zero Trust and micro-segmentation plans now to keep ahead of today's pervasive threats.

While an organisation spends months planning and developing the perfect long-term security roadmap, the threat actors are still circling and the attacks keep coming. As the saying goes, a good plan today is better than a perfect plan tomorrow. Whatever the next step is in your Zero Trust strategy, prioritise action – push for stronger security *now*. ◆

“I love the Now Platform® – it makes work simple. My teams have been able to be much more productive and efficient. Game changer!”

– Tim McDavid, ServiceNow customer



Take work to the next level

servicenow

www.servicenow.com

“With the Now Platform, the sky’s the limit.”

– Stefan Sieger, Head of Customer Experience & Digital Delivery, Group Operations

“The Now Platform delivers the best work setup of any other platforms out there. We’ve tried many organizational methods over the years, but Now goes above and beyond. I couldn’t imagine life without it.”

– James O’Neil, ServiceNow customer

Is AI the answer to the SOC's problems?

Artificial Intelligence has opened many doors for cybersecurity professionals, but it has also caused the attack surface to widen. Geert van der Linden, Cybersecurity Business Lead at Capgemini Group, discusses how SOCs can work smarter to lighten the load with technology and whether AI is the answer for all the SOC's troubles.

Cybersecurity professionals have had a tough time of it recently. Their services have never been more in demand, but equally the cyberthreat landscape has never been more varied and sophisticated. The last 18 months have seen the rise of double extortion ransomware, record-breaking DDoS attack volumes. Any ambitious professional loves a challenge, of course, but there are limits and recent research has shown that three-quarters of security operations staff are feeling the strain.

With the cyberskills shortage a perennial issue – recent research puts the deficit at 3.1 million – clearly Security Operations Centres (SOCs) are not going to be able to simply throw manpower at the problem. They'll have to work smarter, not harder, to lighten the load, and Artificial Intelligence may be the technology capable of doing the heaviest lifting.

Leveraging AI in the SOC

Against this backdrop of stressed-out, time-poor and stretched SOC teams, AI is already being used to try and better manage workloads and alert volumes. This makes sense, as the bread-and-butter tasks of the SOC – threat identification, tracking and remediation – are the sort that AI excels at. They're rote, mundane and time-consuming, the perfect fit for an AI.

With AI automating the majority of this workload, some of the pressure is taken off employees. This is crucial in a landscape that is lighter on skilled cybersecurity professionals and facing an ever-increasing deluge of attacks.

In addition to improving the quality and speed of analysis, AI technologies can also perform threat modelling and impact analysis – activities which have previously relied on the expertise of highly skilled cybersecurity professionals. In fact, AI has advanced so much so that it can provide insights that were previously impossible through solely manual analysis. For instance, some can identify when threats could result in attacks on the corporate network and shut down particular services or subnets based on activities determined to be potentially

harmful. Others can scan vast amounts of code and automate the process of discovering vulnerabilities.

Can AI be the answer for all the SOC's troubles?

While AI can speed up – and scale up – the data analysis process, it's not the ultimate solution. Regardless of developments in the technology, AI simply cannot replace cybersecurity experts.

People often perceive AI as eventually replacing humans. While that can't be ruled out in the future, for now AI still has far too many issues for that to be a reality. By its very nature, AI is another system that can be targeted, which increases the attack surface available to cybercriminals. Such attacks can confuse the underlying Machine Learning model and bypass what the system is intended for. For example, Generative Adversarial Networks (GANs) can be used to fool facial recognition security systems or subvert voice biometric systems.

As we increasingly rely on AI – and therefore give it more responsibility – ethics and privacy need to be taken into account. As AI becomes more advanced, these will only become more important, and just adds to the argument against SOC being solely AI-powered.

> Despite all its advancements, AI can only ever be as good as the data it is fed.

Ensuring fair AI for all

Despite all its advancements, AI can only ever be as good as the data it is fed. In order to maximise accuracy, AI systems require huge volumes of high-quality

Geert van der Linden, Cybersecurity Business Lead at Capgemini Group

training data. But at the same time, this raises the potential of ethical lapses and intrusions of privacy. How much would you let an AI know about you? Would you sacrifice privacy for security?

There are also regulatory hurdles to consider. For example, data from financial services firms or medical sciences organisations are under heavier regulatory scrutiny than other industries. Should they therefore sacrifice cybersecurity by having less effective AI, when the sensitive data they hold is the most tempting for attackers?

If SOCs are to gain the trust of the customers that they're hired to protect, they need to be completely transparent with how much and what kinds of data they're feeding to their AI programs and militant in ensuring those lines are not overstepped.

While AI will likely transform the SOC over the next five to 10 years, security professionals shouldn't start job hunting. In fact, the future success of AI will rely hugely upon the human element. The old game of cat-and-mouse may come to an end, but security professionals will have a new purpose: ensuring their most powerful weapon is being used judiciously and, most importantly, ethically. ◆

Security professionals will have a new purpose: ensuring their most powerful weapon is being used judiciously and, most importantly, ethically.

INTELLIGENT CIO

Providing Unparalleled Technology Intelligence

A Lynchpin Media PUBLICATION

VISIT OUR WEBSITES

GO PHISH

WE 'GO PHISHING' WITH JOHN SMITH, EMEA CTO, VERACODE, WHO TELLS US ABOUT LIFE INSIDE AND OUTSIDE THE OFFICE.

What would you describe as your most memorable achievement in the cybersecurity industry?

My most memorable moment was when I was running an AppSec training course for a customer and an enthusiastic student accidentally shut down a business-critical SQL Server via a SQL Injection vulnerability we had been discussing. In terms of achievement though, I think that my time at Veracode has allowed me to help many customers both large and small with their AppSec challenges over the (almost) 10 years so far. This is my first time at an SaaS vendor company and I was struck right from the beginning by the difference it makes to the relationship when your customers rent your software rather than owning it.

> I find that much of my working life is virtual and never more so than in the last two years so doing something quite different that has a physical result helps me to fully switch off and unwind.

What first made you think of a career in cybersecurity?

Truthfully my first step was entirely a happy accident. I was working as a developer and a former colleague brought me into a security start-up as part of the development team. The thing that has kept me in the security space is the pace of evolution and innovation – both from the attackers and the defenders. These days I think that more than ever I also appreciate the responsibility of cybersecurity. You don't have to look far to see real world examples of the consequences when defences are breached and so the extent to which all aspects of our lives are now entwined with the digital world makes cybersecurity ever more important.

What style of management philosophy do you employ with your current position?

I've been fortunate to have some truly excellent managers over my career so far and one thing they've had in common is that they almost never told me what to do or how to do it – at least not beyond giving me assignments or projects to own. When I needed help, they were happy to coach me and patient enough to let me reach my own conclusions. That's how I try to work with my team.

What do you think is the current hot cybersecurity talking point?

The most recent cybersecurity fire drill has been the Log4J vulnerability which once again highlights the difficulties in managing the security of the software supply chain. This was a hot topic throughout 2021, including the Executive Order. More broadly, I think that the trend of Everything-as-Code will drive a lot of cybersecurity conversations in 2022. When EAC is combined with the rapid deployment of code (i.e., CI/CD) there are huge benefits to enterprise agility but that also brings a new challenge of being able to apply continuous security.

How do you deal with stress and unwind outside the office?

I have a very basic workshop in my garage where I work on various projects, with varying degrees of success. I also enjoy gardening and in particular growing vegetables, again with varying degrees of success. I find that much of my working life is virtual and never more so than in the last two years, so doing something quite different that has a physical result helps me to fully switch off and unwind. It also helps that once in a while I make something that is useful or tasty.

If you could go back and change one career decision, what would it be?

I don't think there's a lot that I would change. That's not because I haven't made any bad decisions – anyone who thinks that is either very lucky or not being honest with themselves – but I don't think that agonising over mistakes (or sub-optimal choices) is helpful. Learn from mistakes and move forward.

> My role has been stable over the last 12 months – building and optimising my team to help our customers gain value from their partnership with Veracode.

What do you currently identify as the major areas of investment in the cybersecurity industry?

One major area of investment in the cybersecurity industry is the growing cybersecurity skills shortage. Companies are increasingly realising the need to invest in ongoing training to meet the demands of the changing workforce and skillset. Even though the number of cybersecurity graduates is expected to double in the next two years in Europe, ENISA already predicts this is not enough to close the skills gap which means it's up to businesses to invest in training and education to close the gap.

Are there any differences in the way cybersecurity challenges need to be tackled in the different regions?

There are, of course, various levels of market and technological maturity in different regions so the challenges are slightly different but I think that the delta has shrunk over time. Global

connectivity has driven that strongly but also cloud technology. Increasingly, we see that software and infrastructure is in the cloud and so the region is less of a determining factor than the particular cloud provider or technology you use.

What changes to your job role have you seen in the last year and how do you see these developing in the next 12 months?

My role has been stable over the last 12 months – building and optimising my team to help our customers gain value from their partnership with Veracode. What has changed and will continue to change is what that value looks like and the stakeholders we are working with.

This is a continuing trend for software security where ownership is transitioning from a pure CISO-led function to a development-led approach. Most organisations are somewhere along this journey but the pace seems to be accelerating and means that we need to move with it.

What advice would you offer somebody aspiring to obtain a C-level position in the security industry?

Don't over-specialise. That's not to say that it's a bad thing to develop deep knowledge of the space you are currently working in but you shouldn't be afraid to branch out and explore domains that are at first glance unrelated. This is true in both a horizontal (different technology domains) and a vertical (strategic vs. tactical) sense. ◆

FOCUS YOUR ATTENTION

A Lynchpin Media BRAND

- CONNECT WITH **PROSPECTIVE** CUSTOMERS
- PRESENT YOURSELVES AS **THOUGHT LEADERS**
- **PROMOTE** YOUR BRAND

The Lynchpin Media video content partner to:
Intelligent CIO | Intelligent CISO
Intelligent Data Centres | IntelligentSME.tech
IntelligentCXO.com | Intelligent Tech Channels

INTELLIGENT BRIEFINGS

For more information, contact jess@lynchpinmedia.com

www.intelligentbriefings.com

FIVE THINGS YOU NEED TO KNOW TO SECURE YOUR WORKPLACE

Murray Mills, Manager – Cyber Security at Tecala, tells us how companies can identify cybersecurity gaps that may require external assistance or additional resourcing.

Murray Mills, Manager – Cyber Security at Tecala

With 2022 now underway it's worth reflecting on the year that was, exploring what we've learned and what can be applied to your strategic planning for the next 12 months.

Last year at Tecala, we drew inspiration from a theme focusing on emerging stronger from what 2020 and the first part of 2021 threw at all of us.

Most organisations spent the year digitally transforming and adopting cloud-based systems to enable work-from-anywhere scenarios. Words like productivity and continuity permeated all technology and business conversations.

But so did security. With workforces distributed and working in new hybrid models, using technology systems they may have been unfamiliar with, an effective security solution for this environment was critical.

Organisations recognised this, but so did attackers. One survey found 73% of Australian organisations fell victim to cyberattacks targeting remote workers in the past year, suggesting far more work is needed to layer additional protections, build resiliency and raise internal security awareness. Ultimately, as Gartner notes, long-term work-from-home 'requires a total reboot of policies and security tools suitable for the modern remote workspace'.

Tecala is already undertaking these kinds of reviews. We use them as the basis for crafting security strategic roadmaps that tailor a security journey to an organisation's specific needs over forward years. The roadmap takes organisations from where they are now to where they want to be; is aligned to key threat mitigation frameworks such as the Essential Eight or the CIS Controls; and is designed to help organisations address the substantial challenges and security headwinds they are now facing.

While every review and roadmap is different, just as every organisation's needs are different, we have identified some common trends among the organisations we work with from a security perspective.

In the interest of openness and intelligence sharing, we've decided to list the top five here as they may be useful in reflecting on your own journeys to date and identifying gaps that may require external assistance or additional resourcing to close in the year ahead.

Security standards will actually become standard

Organisations presently have a range of standard frameworks to choose from and benchmark cybersecurity readiness. These include domestic frameworks like the Essential Eight, as well as overseas ones such as the Centre for Internet Controls (CIS) 18 and the National Institute of Standards and Technology – NIST – framework.

There's considerable repetition and overlap between the different frameworks, such that meeting the requirements of one would likely place an organisation well on the path to complying with the others as well. Whatever framework an organisation chooses, it is likely to serve them well. However, within the small-to-medium enterprise market, the Essential Eight

and CIS Top are currently favoured because they are generally considered more business-friendly.

Only a year ago, awareness of these frameworks was practically non-existent outside of an organisation's security function. Today, however, it is more common to hear even C-level executives discussing the security standards they are endeavouring to meet.

We expect to see these standards become more tightly integrated into ways of doing business. For example, where company A wants to utilise company B's services, they may ask company B to undertake a third-party risk assessment that includes portions of these frameworks. The message is effectively: meet security best practice or we won't connect with you or integrate with your services.

Multi-layered approaches will become the pinnacle of best practice

When organisations undertake reviews and test their alignment to the security standards and frameworks, it quickly becomes apparent that more work is needed to increase levels of protection.

In my mind, the adoption of multi-layered approaches to security go hand-in-hand with the increased use of these frameworks.

Multi-layering isn't about the number of tools an organisation has. Instead, it's about understanding the spectrum of threats and risk levels and creating security processes to effectively mitigate against them. It's an approach to securing the organisation and one that more often than not, leads an organisation down the path of Modern Management.

Modern Management will come into its own

I spent much of 2021 talking about Modern Management and there's a good reason for that: 80% of the projects that we undertook this year were centreed around Modern Management. There's no reason to believe that level of interest won't continue.

Modern Management is an umbrella term for a collection of strategies, services and software that is designed to help businesses to deploy and manage assets in the 'new world'. It can be used to protect employees and the devices and systems they are logged into, regardless of what they are doing, where they are doing it from and what they're working on.

It also ensures that all people and devices requestingauthorisation to connect to an organisation's network or applications meet appropriate security standards before they can login and then that they can only access resources that are appropriate to their level and associated permissions.

To some extent, organisations may still be refining what work in 2022 looks like. We see organisations recruiting for fully-remote workers that will rarely, if ever, attend an office. We also see employees prioritising flexibility over more conventional workplace benefits. With so many future ways of working still up for negotiation, organisations will need to adapt their approach to Modern Management as well. It may have gotten them this far but will require changes to fit with what the workplace of 2022 will look like.

Security awareness reaches the board

The next two trends are related: the increased visibility of cybersecurity issues within organisations and liability challenges that stem from that.

This year, more than any other before it, cybersecurity became an issue for the board of directors and C-level executives.

Ransomware's role in that cannot be under-estimated: executives have now seen enough times the devastating consequences of a successful infection at other similarly-sized and similarly-resourced firms and are far more aware of the risks and levels of sustainable investment and top-down support required to mitigate against these risks and drive a security-first culture internally.

Other drivers are more direct, such as a proposal on the table to make company directors personally liable for cybersecurity incidents.

Directors of Australian financial sector participants also face direct pressure to skill up on cybersecurity: 'Boards need to strengthen their ability to oversee cyber-resilience. Ultimately, boards are expected to have the same level of confidence in reviewing and challenging information security issues as they do when governing other business issues', Australia's corporate watchdog recently wrote.

The intersection of governance and cybersecurity will only increase in importance. Cybersecurity will be a top-down problem that must be taken seriously and for which responsibility will ultimately sit with the board and C-level executives.

It will become harder and more costly to get cyber insurance

On the other side, escalating ransoms and mop-up costs have cyber insurers de-risking as much as possible.
Too many organisations are being compromised and running up multi-million-dollar clean-up bills they expect insurers to meet. Payouts have halved in some cases, while premiums have skyrocketed; industry body CIAB saw cyber premiums rise 27.6% in the three months to September 30 alone.

At the same time, insurers are trimming exclusions, testing contractual clauses before the courts and forcing those seeking cover to constantly improve their baseline security capabilities and technology to reduce the risk of compromise. We have seen during recent cyber insurance renewals that insurance companies are aligning questions to CIS and Essential Eight frameworks.

The alignment to frameworks is catching some companies out when asked to provide evidence of MFA enforcement and vulnerability management capabilities for example.

All of which is to say that cyber insurance is a rapidly evolving space both in Australia and overseas and 2022 will make or break the business models that have brought us to this point.

There may be very real ramifications for the ability of organisations to secure cost-effective cover as a result and that, in turn, is likely to lead to a fresh round of investments in cybersecurity aimed at reducing liability and mitigating against professional and organisational risk all around. ◆

A Lynchpin Media PUBLICATION

@IntDataCentres

IN ASSOCIATION WITH dca The data centre trade association

INTELLIGENT DATA CENTRES

The 'intelligent' data centre focused brand from Lynchpin Media, available in print and digital formats.

Visit us on **intelligentdatacentres.com**

Editorial enquiries Alix Pressley
alix@lynchpinmedia.com
+ 44 20 3026 6825, Ext 1003

Sales enquiries Michal Zylinski
michal@lynchpinmedia.com
+ 44 20 3026 6825, Ext 1002

Most read

01 European oil supply cyberattack causes disruption

02 UK, US and Australia issue joint alert on ransomware attacks

03 KP Snacks victim of ransomware attack

04 More C-suite engagement needed in 2022 to mitigate cyber-risk

05 Study reveals insider threats cost organisations US$15.4 million annually, up 34% from 2020

MARTCx

16 February 2022 **Topgolf, Dubai, UAE**

Adding the X factor to your marketing & customer experience strategies

LEAD SPONSOR

UNIFONIC

PLATINUM | CUSTOMER ENGAGEMENT PARTNER

moengage

PLATINUM SPONSOR

netcore

GOLD SPONSORS

the ENTERTAINER™ — business —

SITECORE®

SUPPORTING PARTNER

EUPHORIA www.euphoria.ae

ORGANISED BY

MARKET SOLUTIONS EVENTS MANAGEMENT

PANEL DISCUSSIONS – TECH PRESENTATIONS – COCKTAILS AND NETWORKING – GOLF BAYS – GAME CORNERS

>spiderSilk;

We identify your attack surface before cybercriminals do.

Discover the unknown unknowns.

REQUEST A DEMO

To find out how we can help you **identify** & **protect** your attack surfaces

RESONANCE
POWERED BY >spiderSilk;

www.spidersilk.com

SAN FRANCISCO | TORONTO | DUBAI