OCT – DEC 2023

SECURITY SOLUTIONS TODAY

PHYSICAL & CYBERSECURITY INTEGRATION

IN THIS ISSUE

CONTACT

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

EDITOR Navkiran Kaur (sst@tradelinkmedia.com.sg)

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

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

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

Vectors/Images Credit: Freepik.com
Designed by Fawzeeah Yamin

SECURITY SOLUTIONS TODAY
is published quarterly by Trade Link Media Pte Ltd (Co. Reg. No.: 199204277K)
1 Paya Lebar Link, #04-01, Paya Lebar Quarter 1 (PLQ 1), Singapore 408533
Tel: +65 6842 2580
ISSN 2345-7112 (E-periodical)

SOPHOS EXCELS IN MITRE ENGENUITY ATT&CK® EVALUATIONS WITH 99% DETECTION COVERAGE

Image by Freepik

Singapore – Sophos, a global leader in innovating and delivering cybersecurity as a service, today announced its strong results in the MITRE Engenuity ATT&CK® Evaluations. Sophos Intercept X with XDR detected 99% of the adversary behaviours in the evaluation, reporting 141 out of 143 adversary attack steps.

Sophos Intercept X with XDR excelled in the independent ATT&CK Evaluations with its comprehensive EDR and XDR capabilities that deliver actionable context on the "what," "why" and "how" of attacker behaviours. In addition, Sophos Intercept X with XDR recorded rich analytic data on 98% of the substeps in the ATT&CK Evaluations.

"As active adversaries continue to prey upon the unprepared, good cybersecurity outcomes increasingly depend upon competent technologies in the hands of skilled operators. MITRE's evaluation is a powerful objective measurement of a technology's ability to produce the fundamental observations and classifications needed to effectively identify and defend against attackers," said Joe Levy, President and Chief Technology Officer at Sophos. "Sophos meticulously architects its solutions for security operators, empowering them with superior protection, detection and response capabilities for known and unknown threats before they become full-blown, destructive attacks, and we believe MITRE's evaluation results demonstrate the robustness of Sophos' real-world security capabilities."

This round of independent ATT&CK Evaluations evaluated the abilities of 30 vendors in detecting and analysing attack tactics, techniques and procedures (TTPs) of Turla, a known Russia-based threat group. Turla leverages novel TTPs and custom tooling to evade security defences, and was chosen as the evaluation adversary based on its innovative stealthy manoeuvres; targeted sectors, including government, critical infrastructure, education, and more; and breadth of open-source reporting on its tradecraft.

"Turla is one of the most sophisticated threat actors, and their tradecraft is platform diverse, dynamic in stealth, and layered in persistence," said Amy Robertson, MITRE cyber threat intelligence lead, ATT&CK Evals. "This round provides an emulation that focuses on kernel and service-level operations that often run with the same permissions as detection and protection products. Our goal is to empower end users and purchasers with unbiased insights into the product capabilities that detect these advanced adversary behaviours, while also collaborating with the participating vendors to evolve their products."

Sophos Intercept X with XDR combines active adversary mitigations – including industry-first Adaptive Attack Protection that immediately activates heightened defences when a hands-on-keyboard attack is detected, stopping the attack and providing defenders valuable additional time to respond; anti-ransomware technology; deep learning artificial intelligence; and exploit prevention to prevent and stop attacks. It is powered by Sophos X-Ops threat intelligence, a cross-operational task force of more than 500 security experts within SophosLabs, Sophos SecOps and SophosAI.

For more information on Sophos' evaluation results, watch this video and visit https://attackevals.mitre-engenuity.org/enterprise/turla/. ■

SOPHOS NAMED THE #1 LEADER FOR MDR AND FIREWALL BY G2

Sophos Ranks Highest in 26 Reports and Earns 114 Award Badges as the Only Leader Across MDR, XDR, EDR, Endpoint Protection, and Firewall

Singapore – Sophos, a global leader in innovating and delivering cybersecurity as a service, today announced it has been named the number one overall global Leader for Managed Detection and Response (MDR) and Firewall Software in G2's Fall 2023 Reports.

Sophos ranks highest in 26 G2 reports spanning global regions and customer market segments based on validated customer reviews. Earning 114 total award badges, Sophos is once again the only Leader across MDR, Extended Detection and Response (XDR) Platforms, Endpoint Detection and Response (EDR), Endpoint Protection Suites, and Firewall Software.

"We take tremendous pride in every customer review because our approach to delivering cybersecurity as a service is driven by our customers' goals, challenges, ideas, and successes," said Raja Patel, senior vice president of products and managed services at Sophos. "Right now, a goal for many organizations is to detect and stop threats faster in response to a growing trend of cybercriminals executing attacks with unprecedented speed.

As detailed in our Active Adversary Report for Tech Leaders, we saw a continued decline in median attacker dwell time, from nine days in 2022 to five days for ransomware attacks in the first half of 2023. Our position as the only Leader across the most critical prevention, detection and response solutions is evidence that we're enabling customers to address this and many other emerging attacker behaviors with speed and efficiency."

Recent Sophos customer reviews on G2 include:

"Seamless integration and proactive protection – Sophos MDR elevates

Vector by Freepik

cybersecurity to the next level: The 24/7 threat hunting service from Sophos MDR stands out as a feature of utmost importance, providing around-the-clock vigilance and prompt reaction to emerging threats. Its true value lies in the managed remediation process – unlike other solutions that merely notify, Sophos steps in to effectively stop and rectify the issue and then informs us about the incident. This proactive and hands-on approach is what sets Sophos MDR apart and makes it a highly appreciated solution," said a vice president of IT at a mid-market company.

"Sophos MDR is a must: My team is small, and it's great knowing if we're all busy putting out IT fires that MDR is ready to take action if my team is unable to respond immediately to suspicious activity. This is much better than relying on alerts that we need to investigate. Of course, we have alerts enabled, but setting the thresholds for the alerts is nearly impossible; the alerts are either not sensitive enough and we'll miss something important, or the alerts are too sensitive, and we receive too many to investigate. Sophos MDR didn't just solve this problem; it completely removed it," said a mid-market customer.

"Proactive threat detection by security experts 24/7: This service freed up our staff to focus more on business enablement, knowing that the MDR team had us covered 24x7 on security. The Sophos Central dashboard provides quick information at a glance, and the support team is there whenever we need additional help," said a mid-market customer

"One of the best endpoint protection (solutions) on the market: Sophos Intercept X actively monitors the latest malware and ransomware for all our PCs, Macs and servers in one cloud-based suite. I love the ease of management that comes with the dashboard," said an IT director at a mid-market company.

"Network security made simple with Sophos Firewall: Sophos Firewall is a robust security solution that offers advanced threat protection, easy management and granular control over your network traffic. Its features help you secure your network, improve network performance, and prevent cyberattacks, making it an ideal choice for businesses of all sizes," said an assistant manager of network administration and cybersecurity at an enterprise company.

These are the latest in a series of industry accolades for Sophos' managed security services and solutions, including Sophos MDR, Sophos Intercept X, Sophos XDR, and Sophos Firewall. These offerings have also this year been named Gartner Peer Insights Customers' Choice for MDR and Network Firewalls, and winners of the Frost & Sullivan Competitive Strategy Leadership Award, CRN Annual Report Card Awards, CRN Tech Innovator Awards, MSP Today Product of the Year Awards, and more. ■

ST. LUKE'S UNIVERSITY HEALTH NETWORK SAFEGUARDS MILLIONS OF PATIENT RECORDS; BOOSTS CYBER RESILIENCE WITH RUBRIK AND MICROSOFT SENTINEL

Healthcare services non-profit achieves over 73 per cent cost savings using Rubrik data security solutions alongside Microsoft Azure and Sentinel.

Singapore – Rubrik, the Zero Trust Data Security™ Company, today announced that St. Luke's University Health Network (St. Luke's) replaced its legacy backup vendor with Rubrik to support its shift to the cloud and achieve cyber resilience. Relying on Rubrik Security Cloud, St. Luke's can now recover from cyberattacks within minutes or hours, as opposed to months.

St. Luke's is a non-profit organisation that provides healthcare services for more than 80,000 patients and more than 340,000 emergency room visits every year across 14 campuses and 300 outpatient sites. St. Luke's houses 2.5 petabytes of data and millions of patient records in Epic, its patient access and medical records system.

Cyber recovery simulations revealed that if St. Luke's were hit with ransomware, patient care would be significantly impacted because it would take months of downtime and millions of dollars to recover. These insights helped St. Luke's recognize its need for a modern data security platform. Since switching to Rubrik, St. Luke's has seen a savings of 73 per cent of the total cost of ownership. Additionally, Rubrik products like Threat Hunting and Anomaly Detection alert St. Luke's to real-time changes in its environment—putting trust in the integrity of its data.

"In our industry, a cyberattack paralyses our ability to provide life-saving care to our patients—so cyber resiliency is not optional," said David Finkelstein, Chief Information Security Officer at St. Luke's. "With Rubrik Security Cloud, we have secured our sensitive data, gained confidence and peace of mind in the resiliency of our operations, and can uphold our commitment to providing outstanding healthcare services even if we face a cyber event."

Vector by Freepik

Backups are an important defence against ransomware. However, the recent Rubrik Zero Labs State of Data Security report found that 90 per cent of external organisations reported that malicious actors attempted to impact data backups during a cyberattack, and 73 per cent were at least partially successful in these attempts.

"Legacy backups are a hunting ground for cybercriminals, as they were historically built for natural disasters — not modern cyberattacks," said Anneka Gupta, Chief Product Officer at Rubrik. "Healthcare organisations with particularly sensitive data must prioritise a strong remediation plan that relies on uncompromised backups. St. Luke's took a proactive stance securing their patient data —and this approach will radically improve their long-term cyber resiliency."

Rubrik and Microsoft: The Backbone of St. Luke's Data Security

St. Luke's systems, namely Epic, needed to be operational around the clock. In order to ensure its data is available at all times, St. Luke's decided to migrate Epic from its on-premises data centre to Microsoft Azure. "Rubrik made it possible for us to move to the cloud and benefit from cutting-edge solutions in Microsoft Azure and Microsoft Sentinel," said Finkelstein. By leveraging Azure, St. Luke's is able to take advantage of the flexibility and cost savings of the public cloud by scaling enterprise applications up or down, depending on demand.

St. Luke's also utilised Rubrik's integration with Microsoft Sentinel, benefitting from a single pane of glass to monitor for threats and quicken cyber investigations. Rubrik expanded its Microsoft Sentinel integration in June 2023, unveiling a joint collaboration to integrate Rubrik Security Cloud with Microsoft Sentinel and Azure OpenAI Service to accelerate cyber recovery through the use of generative AI and Natural Language Processing (NLP).

Read the St. Luke's case study on Rubrik's website to learn more: https://www.rubrik.com/customers/st-lukes-university-health-network.

For more information, please visit www.rubrik.com and follow @rubrikInc on Twitter and Rubrik, Inc. on LinkedIn. ■

CROSS-INDUSTRY CUSTOMER GROWTH AND MULTI-SOLUTION UPTAKE POWER ARMIS' BUSINESS MOMENTUM

Organisations choosing to expand with Armis as they seek one platform for all asset intelligence and security needs.

Image by Freepik

San Francisco – Armis, the asset intelligence cybersecurity company, today announced another business milestone since it reached its $100M ARR milestone in February, announcing it has achieved 80% customer growth in just the first 6 months of its fiscal year, ending July 2023. Customers across the globe also expanded their use of the Armis Platform with a 50% adoption rate of two solutions in the Armis portfolio, with over 15% adopting three or more of its solutions in the past year.

"We focus on empowering businesses with asset intelligence and actionable plans so they can be assured that their infrastructure is safe and operational at all times," said Yevgeny Dibrov, Co-Founder and CEO at Armis. "Today I see Armis chosen as the platform of choice for Fortune 100, 200 and 500 companies all around the world who are looking to understand their attack surface and proactively defend themselves against increased threats. I measure our success not only in financial growth, but in the positive impact that the company is having on virtually all industries thanks to the trust that our customers have given us."

The Attack Surface is Expanding and Threats are on the Rise

Armis expects that by 2025, the number of connected assets will grow to 50B but 80% of assets remain unseen, unmanaged and lacking in any security measures. Vulnerabilities are also increasing with a growth of 689% in the last 6 years, many targeted at critical infrastructure with cyberattacks specifically up 140% in this sector. This increase has created a fast-changing and difficult situation in which organisations are struggling to stay ahead. Armis is solving customers critical cybersecurity challenges with four key offerings:

1. OT/IOT security - See and secure OT/IOT networks and physical assets, ensure uptime and build an effective & comprehensive security strategy
2. Medical device security - Complete visibility and security for all medical devices, clinical assets and the entire healthcare ecosystem - with zero disruption to patient care
3. Asset management and security - Complete asset inventory of all asset types allowing any organisation to see and secure the attack surface
4. Vulnerability prioritisation and remediation - Consolidate, prioritise and remediate all vulnerabilities; improve mean time to remediation (MTTR) with automatic remediation and ticketing workflows

These four solutions, all recognized by analysts and customers, are all built on top of the same platform ensuring customers can benefit from an integrated platform which unlocks value and enables customers to truly see, protect and manage their attack surface.
Armis becomes the cybersecurity industry standard, protecting the most critical assets on the planet
Some notable recent wins include Vestas, the leading manufacturer and service provider for sustainable wind energy in the world, Reckitt, the multinational consumer goods company, Booking Holdings, the world leader in online travel, the Port of Antwerp, the world's largest cargo port and JLR, the biggest luxury vehicle manufacturer in the UK.

continue on page 8

"As a leading manufacturer and service provider for sustainable wind energy, our customers require a high degree of security controls to meet regulatory requirements. We utilise Armis to detect and respond to threats and have worked extensively with Armis to shape the integration, so the product fits into our overall detect and response strategy. The insights provided by Armis have proven highly valuable in day-to-day operations again and again, and we are currently expanding our installation," said Steffen Høgh Vinter, Director CMRC Enablement and Problem Management, Vestas.

"When we started the program from a central cyber team, we had no visibility into our factory so every device was unseen. Now, with Armis deployed in half our factories, we've seen 10s of 1000s of devices that we didn't know about before. Armis is allowing us to address three use cases: firstly, giving us that visibility that we didn't have before. Secondly, allowing us to identify vulnerabilities, which allows us to de-risk our state. And thirdly allows us to identify any unusual behaviour that's happening in our network," said David Boyd, Director of Cyber Strategy & Engagement at Reckitt.

"Armis is one of those inventions that simply needed to happen. It meets a foundational, unmet need in cybersecurity, namely the ability to "see all evil" (on the network) by discovering rogue devices and providing real time intelligence about their identity and condition. With Armis, there's no need for an army of engineers or analysts to decipher complex systems and their signals," said Spencer Mott, Chief Security Officer, Booking Holdings.

Analyst Recognition and Accolades

In 2023, Armis was recognized both in the Deloitte Technology Fast 500™ for its growth and high performance, and by Fast Company as the most innovative security company of 2023. Additionally, it has been named an honoree to the Inc. 5000 list, and its Armis Partner Experience Program (APEX) was given a 5 star rating in the 2023 CRN Partner Program Guide.

- Armis is recognized as Leader in the 2023 GigaOm Radar for Operational Technology Security.
- Armis is recognized as a Representative Vendor in three 2023 Gartner Market Guides: Gartner Market Guide for CPS Protection Platforms, Gartner Market Guide for Medical Device Security Solutions, and Gartner Market Guide for Vulnerability Assessment.
- Armis is named as a Sample Vendor in five 2023 Gartner Hype Cycles:
  - Hype Cycle for Security Operations, 2023
  - Hype Cycle for Workload and Network Security, 2023
  - Hype Cycle for Cyber Risk Management, 2023
  - Hype Cycle for Digital Grid Transformation Technologies, 2023
  - Hype Cycle for Real-Time Health System Technologies, 2023
- KLAS Research recognizes Armis as a top performer of fully-rated vendors in the Healthcare IoT Security 2023 report and the highest rated cross-industry vendor.
- Armis has been named a Visionary in the Vendor Vision Report for RSA 2023 by Enterprise Management Associates (EMA).

For more information, please visit armis.com or e-mail at info@armis.com. ■

NEARLY 16,000 REGISTRANTS FROM 95 NATIONS PARTICIPATE IN GSX 2023

Three-day event delivered 200+ education sessions and showcased 470+ leading innovators in security solutions.

Alexandria, VA/Dallas, TX – Global Security Exchange (GSX) 2023 has concluded at the Kay Bailey Hutchison Convention Center in Dallas, Texas. Presented by ASIS International, the world's largest association for security management professionals, the event offered discussion and idea exchanges for the global security community. Attendance exceeded projections, with nearly 16,000 registrants from 95 countries along with more than 470 exhibitors demonstrating the latest security solutions.
"I couldn't be prouder of the success of our annual conference and trade show. GSX is not just an event; it's a testament to the passion, dedication, and collective brilliance of our members and ASIS staff," stated Tim McCreight, CPP, 2023 President, ASIS International. "Together, we've created a truly remarkable experience for security professionals across the globe that will have a long-lasting impact."

continue on page 11

This year, GSX was supplemented by a weekend of pre-conference events, such as Secure Horizons: An Immersive Experience for Senior Security Executives, ASIS Volunteers' Day, and the ASIS Awards of Excellence alongside the Outstanding Security Performance Awards (OSPAs).

GSX kicked off on Monday 11 September commemorating 9/11 and a keynote presentation from current member of the European Parliament, Radek Sikorski. Sikorski's presentation titled "Securing Democracy Worldwide: Why We Must Win" discussed the threat Putin poses not only to Ukraine, but also to Poland, Europe, and democracy at large. Sikorski urged both the European Union and the United States to support the efforts in Ukraine.

Following Sikorski's keynote presentation, the event's exhibit hall opened – showcasing more than 470 industry leaders from three continents. Monday also launched the start of 218 education sessions over this three-day event.
In Tuesday's general session, President George Bush discussed his time in office, conflict abroad, and the 9/11 attacks. President Bush also shared his thoughts on the most pressing issues facing the United States today, and the effectiveness a president can have when dealing with those issues.

Tuesday featured a speed mentoring session that allowed members of ASIS who are looking to further develop their career to meet with more experienced security practitioners who can help them advance their career. The speed mentoring session featured participants from across five continents.

On Tuesday, the World Security Report 2023, commissioned by Allied Universal and their international business G4S, was unveiled. The report offers a groundbreaking look at the concerns of nearly 1,800 chief security officers from large, global companies in 30 countries representing a combined annual revenue of more than $20 trillion in 2022.

The final day of GSX, Wednesday 13 September, celebrated Military and Law Enforcement Appreciation Day and featured former CIA Officer and FBI Special Agent Tracy Walder. In her keynote address, Walder identified what she sees as the three most urgent threats facing the United States: fragile states, China, and domestic terrorism. As a thank you to all active duty and veteran military, law enforcement, and first responders, these groups were invited to attend GSX for free this day.

On Wednesday, ASIS announced a tool and supporting materials developed by the ASIS Professional Certification Board and the ASIS Military Liaison Community that will help active-duty military and veterans translate the skills they learned in the military to work in the private security sector. The initial launch began with the U.S. Army; however, the tool will soon be expanded to serve other branches of the U.S. military, and later law enforcement and other global military branches as well.

GSX featured SM Live, which took the form of a series of interviews with industry leaders conducted by editor-in-chief of ASIS International's award-winning publication Security Management, Teresa Anderson. SM Live spotlighted 17 discussions with industry leaders and innovators on topics ranging from cybersecurity, to professional development, to school security. Those discussions can be viewed here.

GSX 2023 highlighted three Game Changer sessions with industry experts who provided lively presentations on ethics, navigating global mistrust, and the impact of global crises on security.

Among the robust learning opportunities at GSX, the event featured a number of "speed learning" sessions, such as the X Stage, which featured cutting-edge solutions that actively shape the future of the security profession. The UnCrewed U Stage offered 14 short, twenty-minute sessions and product demos of the latest uncrewed aircraft platforms, counter UAS systems, and ground-based robots. The Cybersecurity Pavilion addressed topics ranging from the convergence between physical and cybersecurity to artificial intelligence. At Career HQ, security professionals were offered resume reviews, access to the headshot studio, and professional development sessions.

"GSX is a global gathering of thought leaders and industry disruptors and underscores ASIS International's dedication to excellence in education while presenting the most recent advancements in the security sector." said Peter O'Neil, FASAE, CAE, CEO, ASIS International. "With a world-class educational lineup, networking events and opportunities to meet with industry-leading solution-providers, we are proud to advance the security profession in meaningful ways."

GSX delivered opportunities to earn Continuing Professional Education (CPE) credits:

- All-Access Pass (in-person or digital): 22 CPEs
- One-Day Pass (in-person and digital): 8 CPEs for Monday and Tuesday; 6 CPEs for Wednesday
- Expo-Only Pass: 3 CPEs
- Exhibitors: 3 CPEs
- Pre-Conference Review Program Attendees: 13.5 CPEs per program (APP, CPP, PSP)
- According to Visit Dallas, GSX 2023 generated both a direct and indirect economic impact of more than $35 million and supported 7,000 jobs in Dallas.

For more information, please visit gsx.org. ■

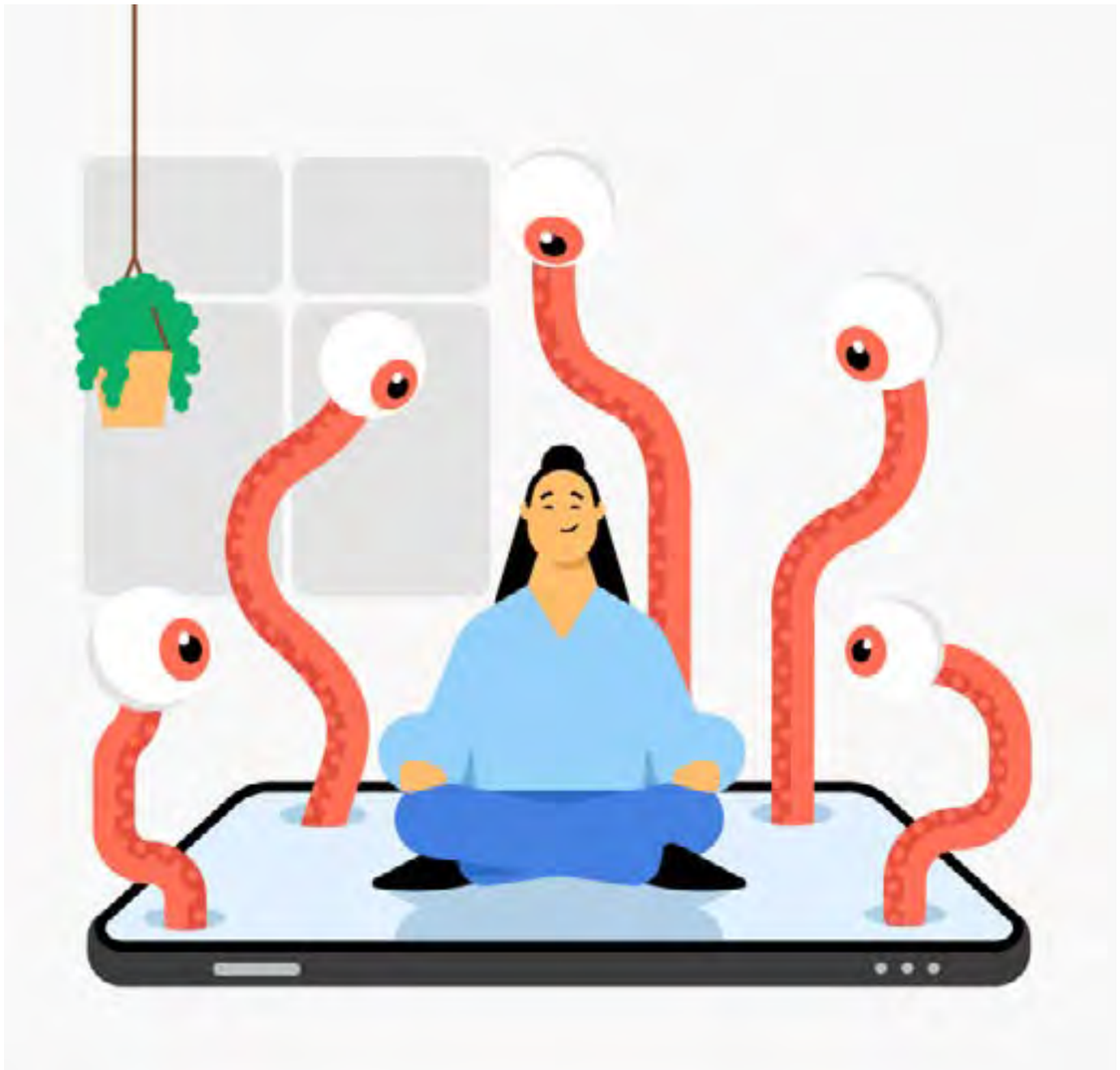
96% OF PEOPLE USE TECHNOLOGY TO UNWIND, FORGETTING ABOUT POSSIBLE CYBERSECURITY RISKS

People mostly relax by watching TV, listening to music, and streaming TV shows or other videos online.

Cybersecurity experts are alarmed because most people use their devices as a relaxation tool. In fact, the latest survey performed by Cint and commissioned by cybersecurity company NordVPN showed that 96% of people turn to technology for relaxation during the day.

While watching Netflix or scrolling Instagram can help alleviate stress, it may also eliminate users' privacy awareness.

Sixty percent of respondents said they turn to their gadgets a few times a day to relax, and 21% said they do so at least once a day.



In which ways do you unwind or relax using devices?	
Watching TV	65.9%
Listening to music	62.9%
Streaming TV shows, movies or watching videos (e.g, on YouTube, TikTok)	52.4%
Scrolling through social media	45.7%
Text messaging (via apps, SMS) or talking to friends/family through voice or video calls	39.1%
Reading or listening to the news	38.8%
Gaming	34.7%
Online shopping	32.9%
Walking or working out using physical health apps (such as Pulsebit, MyFitnessPal, or Google Fit)	20.8%
Reading e-books	18.1%
Using mental health apps (such as Fabulous, Breeze, Calm, or Headspace)	6.8%
Using the metaverse	3.6%

TVs and smartphones are the two top gadgets that people use to relax

In most countries, TV remains the #1 device for relaxation and easy entertainment (70%).

"In the past, very few cybersecurity issues were associated with the use of television. However, now many people use smart TVs. In 2019, the FBI released a warning stating that smart TVs can make users vulnerable to surveillance and attacks by bad actors. Since then, user security technology has become more advanced, but internet-connected devices remain vulnerable," says Adrianus Warmenhoven, a cybersecurity expert at NordVPN.

Warmenhoven is also worried because smartphones are the second most used item for relaxation (69% globally).

"When people are relaxed, they often forget about possible cybersecurity risks. Smartphones are especially at risk because today, no other gadget knows more about its user. That makes smartphones a very appealing target for hackers," says Warmenhoven.

How do people relax using their gadgets?

Two-thirds of respondents choose to unwind by watching TV, and a similar number of people choose to do so by listening to music. More than half of respondents also relax by streaming TV shows or movies or watching videos (e.g., on YouTube or TikTok).

The fourth most popular way of relaxing was scrolling through social media, and 45.7% of respondents admitted to doing so. More than a third also said they feel more relaxed after talking to their loved ones online, gaming, or reading or listening to the news.

How to safely relax using tech

Cybersecurity expert Adrianus Warmenhoven shares some tips that will help eliminate the stress of being hacked for those who use technology to unwind:

- **Keep apps and the phone's operating system (OS) up to date.** Don't skip software updates.
- **Use cybersecurity tools.** Every device you use should have at least an antivirus, a VPN, and a password manager installed if that is possible. That will drastically lower the risk of being hacked.
- **Do your research.** Never download unknown apps — read up on them and make sure they have been developed by a legitimate company.
- **Avoid unofficial app stores.** They're more likely to contain malware-ridden apps.
- **Avoid using unknown Wi-Fi.** And always use a VPN when you do.
- **Be vigilant.** Don't click on suspicious links, don't give out your number to strangers, and be wary of unknown numbers.

For more information, please visit nordvpn.com. ■

JUMIO NAMED A REPRESENTATIVE VENDOR IN FIFTH CONSECUTIVE GARTNER® MARKET GUIDE FOR IDENTITY VERIFICATION

The Market Guide discusses growing concerns about AI-enabled attacks using deepfakes, offers comprehensive market recommendations for security and risk management leaders responsible for identity and access management and fraud detection.

Singapore – Jumio, the leading provider of automated, end-to-end identity verification, risk assessment and compliance solutions, has been recognized as a Representative Vendor for the fifth consecutive time in the latest Gartner Market Guide for Identity Verification,[1] published on September 7, 2023.

Jumio was named as a Representative Vendor among other identity verification vendors. "The listed vendors in this research represent what's core in the market, what extends it and what will transform it," stated the Market Guide.

[1]*Source: Gartner Market Guide for Identity Verification, Akif Khan, 7 September 2023.*

Note: The report title was changed from Market Guide for Identity Proofing and Corroboration to Market Guide for Identity Proofing and Affirmation in 2020 and changed to Market Guide for Identity Verification in 2023.

Disclaimer: Gartner does not endorse any vendor, product, or service depicted in its research publications and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner's research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

Vendors were selected on the basis of one or more of the following criteria:

- Vendors offering capabilities that support identity verification in ways that are unique, innovative and/or demonstrate forward-looking product strategies.
- Frequent inquiries by Gartner clients about a particular vendor for identity verification use cases.
- Vendors that represent particular market segments or geographic regions, thus helping to illustrate the breadth of the market.
- Fair representation from year to year, with rotation of vendors that may have previously met the above requirements, but were omitted simply due to space restrictions.

As defined in the Market Guide, "the purpose of identity verification is to establish confidence in the identity of a user during a digital interaction. As a result, across all geographies and industries, the use cases in which identity verification is required in the market today have become broad in scope. This is accelerating as the pace and reach of digital transformation continue to expand the scope of digital interactions for both customers and workforce."

The Market Guide also highlights growing concerns around generative AI and deepfake technologies, with Gartner reporting a significant increase in clients asking about the integrity of identity verification now that attackers could be using deepfakes.

"Security and risk management leaders must make deepfake detection a key requirement, and should be suspicious of any vendor that is not proactively discussing its capabilities in this respect," the Market Guide states.

"We think that the Market Guide reinforces what we believe to be true: that the rise of deepfakes warrants a stronger form of identity verification, and that organizations must adopt multimodal biometric authentication, multi-modal liveness checks, deepfake detection models, as well as technologies to prevent presentation and injection attacks," said Stuart Wells, chief technology officer at Jumio.

Jumio was also recently recognized as a Representative Vendor in the 2023 Gartner Market Guide for User Authentication, published on August 23, 2023.

For more information, please visit jumio.com. ■

ARMIS LAUNCHES ARMIS CENTRIX™, THE AI-POWERED CYBER EXPOSURE MANAGEMENT PLATFORM

Armis Centrix™ enables organisations to see, protect and manage all physical and virtual assets ensuring the entire attack surface is both defended and managed in real time.

San Francisco – Armis, the asset intelligence cybersecurity company, today announced the launch of Armis Centrix™, the AI-powered cyber exposure management platform. Armis Centrix™ is a seamless, frictionless, cloud-based platform that proactively secures all your assets, remediates vulnerabilities, blocks threats and protects your entire attack surface.

Image by Freepik

Armis Centrix™ enables organisations to discover, contextualise, enrich and profile every asset in their environment whilst also building a line of defence by leveraging Armis Centrix™ Asset Intelligence risk scores, policies, alerting and visualisations and most importantly: prioritise efforts against the exposures that matter to your business. Armis Centrix™ also integrates with existing enforcement and ticketing tools to establish end-to-end workflows and true risk lifecycle management and track risk reduction efforts to easily report on progress made. Armis Centrix™ takes proactive measures, detects threats & stops attacks to establish operational workflows and track risk reduction.

"In a perimeter-less world, where assets are digitally connected, traditional cybersecurity boundaries no longer exist. Legacy on-premise systems and point solutions are no longer fit for purpose leaving your attack surface and most critical assets open and exposed to cyber criminals and multiple bad actors," said Nadir Izrael, CTO and Co-Founder, Armis. "The sheer scale and dynamic nature of the attack surface necessitates an entirely different, AI-driven approach, and that's what Armis Centrix™ is - the AI that powers a suite of powerful tools for managing cyber risk exposure."

Armis Centrix™ helps organisations see, protect and manage their entire attack surface, continuously safeguarding their mission-critical assets from cyber threats. Born in the cloud and fueled by AI, only Armis Centrix™ delivers a truly modular approach to cyber exposure management covering the most critical cybersecurity needs for our clients across 4 solutions:

- OT/IOT security - See and secure OT/IOT networks and physical assets, ensure uptime and build an effective & comprehensive security strategy
- Medical device security - Complete visibility and security for all medical devices, clinical assets and the entire healthcare ecosystem - with zero disruption to patient care
- Asset management and security - Complete asset inventory of all asset types allowing any organisation to see and secure the attack surface
- Vulnerability prioritisation and remediation - Consolidate, prioritise and remediate all vulnerabilities; improve mean time to remediation (MTTR) with automatic remediation and ticketing workflows

"This is a revolutionary advancement that will change the way in which companies answer key questions regarding their cybersecurity posture," said Dana Gilboa, Chief Product Officer, Armis. "Armis can help organisations mitigate their cyber asset risks and protect the entire attack surface by providing the needed intelligence to align security and business efforts. With this approach, we can ultimately provide organisations with the peace of mind they need, allowing them to see, protect and manage all their critical assets."

Armis Centrix™ is industry-agnostic, allowing Manufacturing, Health and Medical, Information Technology, Energy and Utilities, Financial Services, Transportation, Telecommunications and Media, Public Sector and many more to benefit from its capabilities. Additionally, Armis collaborates with the world's premier global technology vendors to ensure its customers can seamlessly integrate Armis Centrix™ with existing IT and security stacks.

For more information, please visit armis.com/centrix or contact us at info@armis.com. ■

ARMIS IDENTIFIES THE RISKIEST ASSETS INTRODUCING THREATS TO GLOBAL BUSINESSES

Data demonstrates a clear need for comprehensive security strategies that account for all managed and unmanaged connected assets.

Singapore – Armis, the leading asset visibility and security company, today released new research identifying the riskiest connected assets posing threats to global businesses. Findings highlight risk being introduced to organisations through a variety of connected assets across device classes, emphasising a need for a comprehensive security strategy to protect an organisation's entire attack surface in real-time.

"Continuing to educate global businesses about the evolving and increased risk being introduced to their attack surface through managed and unmanaged assets is a key mission of ours," said Nadir Izrael, CTO and Co-Founder of Armis. "This intelligence is crucial to helping organisations defend against malicious cyberattacks. Without it, business, security and IT leaders are in the dark, vulnerable to blind spots that bad actors will seek to exploit."

Armis' research, analysed from the Armis Asset Intelligence Engine, focuses on connected assets with the most attack attempts, weaponized Common Vulnerabilities and Exposures (CVEs) and high-risk ratings to determine the riskiest assets.

Assets With The Highest Number of Attack Attempts

Armis found the top 10 asset types with the highest number of attack attempts were distributed across asset types: IT, OT, IoT, IoMT, Internet of Personal Things (IoPT) and Building Management Systems (BMS). This demonstrates that attackers care more about their potential access to assets rather than the type, reinforcing the need for security teams to account for all physical and virtual assets as part of their security strategy.

Top 10 device types with the highest number of attack attempts:

- Engineering workstations (OT)
- Imaging workstations (IoMT)
- Media players (IoT)
- Personal computers (IT)
- Virtual machines (IT)
- Uninterruptible power supply (UPS) devices (BMS)
- Servers (IT)
- Media writers (IoMT)
- Tablets (IoPT)
- Mobile phones (IoPT)

"Malicious actors are intentionally targeting these assets because they are externally accessible, have an expansive and intricate attack surface, and are known weaponized CVEs," said Tom Gol, CTO of Research at Armis. "The potential impact of breaching these assets on businesses and their customers is also a critical factor when it comes to why these have the highest number of attack attempts. Engineering workstations can be connected to all controllers in a factory, imaging workstations will collect private patient data from hospitals and UPSs can serve as an access point to critical infrastructure entities, making all of these attractive targets for malicious actors with varying agendas, like deploying ransomware or causing destruction to society in the case of nation-state attacks. IT leaders need to prioritise asset intelligence cybersecurity and apply patches to mitigate this risk."

Assets With Unpatched, Weaponized CVEs Vulnerable to Exploitation

Researchers identified a significant number of network-connected assets susceptible to unpatched, weaponized CVEs published before 1/1/2022. Zooming in on the highest percentage of devices of each type that had these CVEs between August 2022 and July 2023, Armis identified the list reflected in Figure A. Unpatched, these assets introduce significant risk to businesses.

Assets with a High-Risk Rating

Armis also examined asset types with the most common high-risk factors:

- Many physical devices on the list that take a long time to replace, such as servers and Programmable Logic Controllers (PLCs), run end-of-life (EOL) or end-of-support (EOS) operating systems. EOL assets are nearing the end of functional life but are still in use, while EOS assets are no longer actively supported or patched for vulnerabilities and security issues by the manufacturer.
- Some assets, including personal computers, demonstrated SMBv1 usage. SMBv1 is a legacy, unencrypted and complicated protocol with vulnerabilities that have been targeted in the infamous Wannacry and NotPetya attacks. Security experts have advised organisations to stop using it completely. Armis found that 74% of organisations today still have at least one asset in their network vulnerable to EternalBlue – an SMBv1 vulnerability.
- Many assets identified in the list exhibited high vulnerability scores, have had threats detected, have been flagged for unencrypted traffic or still have the CDPwn vulnerabilities impacting network infrastructure and VoIPs.
- Half (50%) of pneumatic tube systems were found to have an unsafe software update mechanism.

Additional research from Armis is available on the riskiest OT and ICS devices across critical infrastructure industries as well as the riskiest medical and IoT devices in clinical environments.

For more information, please visit www.armis.com. ■

continue on page 17

TDSI LOWERS PRICE ON A SELECTION OF GARDIS ACCESS CONTROL UNITS AND READERS TO SUPPORT CUSTOMERS DURING ECONOMIC CHALLENGES

Prices reduced on best-selling GARDiS products in response to Supply Chain Improvements.

Poole, UK – Integrated Access Control and Security manufacturer TDSi announces a price reduction on a selection of its best-selling GARDiS Access Control Units and Readers. Driven by recent improvements in TDSi's supply chain, the price reductions are designed to help and support installers and end users in a challenging economic climate.

John Davies, Managing Director at TDSi commented, "When we launched our Price List for 2023 at the tail end of last year, it reflected the effect that the global financial pressures of high inflation, energy costs and supply side constraints were having on our business. Regrettably, we were forced at the time to raise some of our prices but were fully aware this would put extra pressure on our customers and were determined to lower these essential increases as soon as possible. With these market forces having now improved significantly, we are very pleased to be able to do that and to pass on the savings benefits to our customers and end users as part of our ongoing commitment to supporting security wherever it is needed."

The MSRP and Trade Price Reductions have been applied to the following best-selling GARDiS Products:

- 5002-6001 – GARDiS G1 Web Embedded Access Control Unit
- 5002-6011 – GARDiS G1 Web Embedded Access Control Unit with Case and Power Supply Unit
- 5002-0600 – GARDiS Proximity Reader
- 5002-0610 – GARDiS MIFARE CSN Reader

TDSi's best-selling GARDiS Web Embedded Access Control Unit is designed to provide seamless and secure access control management. This innovative unit combines the power of an embedded server (removing the requirement for a dedicated PC) with robust access control features, allowing users to conveniently control and monitor access. With its web-embedded interface, administrators can easily configure and manage user permissions, schedules, and event logs, streamlining the access control process.

For more information, please e-mail sales@tdsi.co.uk or visit www.tdsi.co.uk. ■

LEADING TURKISH UNIVERSITY USES IDIS VIDEO TO STREAMLINE COMPLEX SURVEILLANCE SYSTEM

Upgraded 350-camera system transforms security for Social Sciences University of Ankara (ASBU).

Turkey, Ankara – IDIS Solution Suite VMS from the largest manufacturer of trusted South Korean-made video tech, has streamlined operations and transformed security for the Social Sciences University of Ankara (ASBU), Türkiye. ASBU's historic city centre location, with its night-time economy, makes it the study destination of choice for around 5,500 students annually. But with such a busy site, the university also has to deal with an increased risk of incidents, including crime and anti-social behaviour. A 350-camera surveillance system, monitored 24/7 from ASBU's dedicated control room, had been expanded several times over the years. But the resulting mix of six different vendor brands had left the VMS struggling, with froze live images, a hard-to-manage data burden, and difficult to use controls.


Image by Freepik

IDIS integration partner 11S Savunma Sanayi ve Güvenlik Sistemleri was asked to devise the best upgrade route. In an on-site proof of concept demonstration, the company showed how IDIS's VMS, IDIS Solution Suite, (ISS Expert) could quickly register all the mix-and-match cameras and devices, including recorders and a 3x3 video wall.

With the project now completed, the result is elminated complexity allowing seamless control, full functionality of all cameras regardless of the brand, and transformed ease-of-use for operators. They can now control the system from their workstations as well as from the video wall, with browser features allowing the university's fire system to display on the same screen. IDIS MapVue is also being added, with a schematic showing the locations of the cameras, to improve domain awareness and make navigational playback easier.

The IDIS solution is easy to maintain and expand, and a further 100 cameras will be added in the next phase of the project when two renovated accommodation buildings will also benefit from upgraded surveillance. The new cameras will include IDIS 12MP Fisheyes and domes, which are ideal for the historic setting where ceiling heights are up to 9m, and where full coverage with HD image capture is needed, with minimal structural modifications.

To save bandwidth and reduce the storage burden, cameras in corridors, the basement, and other key areas have been set to record only when motion is detected, using a combination of IDIS Motion Adaptive Transmission, and ONVIF motion detection on the other brands.

ASBU's security team can now easily comply requests from law-enforcement agencies for video evidence. Bookmarked event recording makes it easy for ASBU operators to skip from scene to scene when reviewing recordings. And in the next project phase, IDIS Deep Learning Analytics (IDLA) tools will be added for even faster, automated footage review. The IDIS solution also makes it easy and affordable to expand the system, for example with IDIS 310D servers that will allow more cameras to be added and increase storage capacity to ensure longer retention periods without increasing storage costs thanks to IDIS Intelligent Codec.

"IDIS Solution Suite solved all the problems we had with our complex and ageing system, with an easy upgrade that extends the life and performance of all our cameras," says Zafer Buldu, Manager of Hardware & Technical Services, ASBU.

Koray Ozyildirim, IDIS Turkey Country Manager said: IDIS Solution Suite has turned ASBU's cluttered and failing system into a powerful, integrated surveillance solution that is easy to use, adapt, and upgrade, with the assurance of an extended lifespan backed by industry-best warranties."

For more information, please visit www.idisglobal.com. ■

IPC'S CONNEXUS CLOUD EARNS FINANCIAL SERVICES CLOUD AWARD AT THE 2023 SBR TECHNOLOGY EXCELLENCE AWARDS

The cloud solution garners recognition for its expansive and secure trading communications network.

As global markets continue to expand, staying connected for effective communication within the financial trading supply chain has become even more important for efficient trade execution, order routing, and market data delivery. Recognising this opportunity, IPC Systems launched the Connexus Cloud ecosystem, a network connecting more than 7,000 capital market participants in 750 cities across 60 countries worldwide.


Image by Freepik

Entities such as buy-side firms, inter-dealer brokers, liquidity venues, energy firms, sell-side firms, trade lifecycle providers, and clearing and settlement firms have adopted the Connexus Cloud platform to access 550+ public clouds as well as private and hybrid clouds for reliable, high-performance, electronic and voice communications for financial markets participants.

This innovation earned IPC Systems the Cloud-Financial Services Award in this year's SBR Technology Excellence Awards. The awards programme recognises the strides companies in Singapore have undertaken to provide ground-breaking products and services enhanced by digital capabilities.

"We are thrilled to see the Connexus Cloud ecosystem recognised for its ability to facilitate efficient and secure communications within the financial trading supply chain," said Bruce Maslen, Vice President, Asia-Pacific Sales, IPC Systems. "As the industry landscape evolves, we remain committed to innovating and enhancing our offerings to meet the changing needs of financial organisations. Connexus Cloud exemplifies our dedication to providing a unified, high-performance solution that empowers market participants."

Financial transactions remain private and secure thanks to Connexus' robust extranet. The security protocols, size and composition of IPC's global trading community render the Connexus Cloud an effective end-to-end buy-side solution.

IPC continues to enhance and expand the Connexus Cloud ecosystem with innovations that adapt to evolving market conditions and trader expectations and requirements. In April 2022, IPC launched Connexus ALPHA, a high-performance cloud-edge solution integrated into the Connexus Cloud platform. It enables hedge funds, funds of funds, proprietary trading firms, market makers, broker/dealers and other market participants to connect to key global liquidity venues via ultra-low latency optimised point-to-point optical fibre connections. Market participants leveraging Connexus ALPHA gain a valuable speed advantage in executing complex trading strategies whilst reducing the cost of trades.

IPC Systems has incorporated range and versatility into the Connexus Cloud solution, creating a multi-cloud, multi-product ecosystem that supports FIX messaging, multiple transaction standards, unicast/multicast market data, all voice trader circuit types and numerous other industry protocols. The breadth and versatility of the Connexus Cloud solution set it apart from other providers as a global hub linking the community of capital market participants.

In November 2022, IPC Connexus Cloud was awarded 'Best Cloud Provider to the Buy Side' in the 2022 Waters Technology Buy-side Awards. This award highlights IPC's commitment to continuous development and delivery of cutting-edge solutions for the financial markets community.

IPC's Connexus Cloud is a testament of the company's dedication to meeting the evolving needs of financial organisations, providing a secure, efficient, and versatile ecosystem for capital market participants worldwide.

The SBR Technology Excellence Awards is presented by Singapore Business Review Magazine. To view the full list of winners, click here. If you want to join the 2024 awards programme and be acclaimed for your company's outstanding contributions in pursuit of technological innovation, please contact Jane Patiag at jane@charltonmediamail.com. ■

SINGAPOREANS HAVE THE HIGHEST GLOBAL SCORE IN TERMS OF CYBERSECURITY KNOWLEDGE

The study shows that the world's online privacy and cybersecurity awareness is declining.

- The majority of Singaporeans know how to create strong passwords.
- People in Singapore know nothing about online tools that protect digital privacy.
- Around 20% of the Singaporean population are Cyber Stars (very knowledgeable in the field).

Singaporeans are 1st in the world in terms of cybersecurity and internet privacy knowledge, according to new research by the cybersecurity company NordVPN. Singaporean participants have the most Cyber Stars compared to other countries. Cyber Stars know a lot about cyber threats and have a high National Privacy Test score.

The annual National Privacy Test (NPT) is a global survey aimed to evaluate people's cybersecurity and online privacy awareness and educate the general public about cyber threats and the importance of data and information security in the digital age. It gathered 26,174 responses from 175 countries this year.

"By engaging in the National Privacy Test, we aim to cultivate a community of privacy-conscious individuals who actively champion data protection. This initiative aligns with our vision to build a safer, more resilient digital landscape for now and future generations," says Marijus Briedis, chief technology officer (CTO) at NordVPN.

Here are the countries in the **top 3 spots** with the best internet privacy and cybersecurity awareness:

1. Poland and Singapore (64/100)
2. Germany and the United States (63/100)
3. The United Kingdom, Austria, and Portugal (62/100)

However, results show that the world's online privacy and cybersecurity awareness is declining every year.

"With the growing complexity of online threats, it is not that surprising that the world's online privacy and cybersecurity awareness has been on the decline. Paradoxically, the more security solutions there are out there, the worse the results get every year. Raising awareness about the potential risks and educating users about best practices should be at the forefront of our efforts," says Marijus Briedis, CTO at NordVPN.

Singaporeans create strong passwords but fail with tools that protect digital privacy

Research shows that Singaporeans are good at creating strong passwords (98%) and know how devices get infected with malwares (94%). They also know what kind of sensitive data they should avoid sharing on social media (93%), or how to deal with suspicious streaming service offers (91%).

However, only 8% of Singaporeans are knowledgeable about online tools that protect digital privacy, and only one out of 10 know what data ISPs collect as part of the metadata.

Among the Singaporean people, 1% of them are Cyber Wanderers (barely know anything about internet privacy and cybersecurity), while 20% scored 75-100 points and were identified as knowledgeable Cyber Stars.

How have Singaporeans' results changed since 2021?

Globally, more participants consider reading terms of service important this year. However, in Singapore, this understanding increased significantly from 24% in 2021 to 56% in 2023.

The same applies to dealing with phishing attacks. Just under half of respondents (48%) know how to handle phishing attacks in 2021, with a much higher proportion (65%) answering this question correctly in 2023.

When asked what they'd do if their information was exposed due to a data breach, 45% answered correctly in 2021. This year, many more (57%) got it right. The answer is, of course, to check your account for suspicious activity and change your password.

South Korea and Japan were two lowest-scoring countries among the 25 countries analysed

As for other Asian countries, South Korea is the lowest-scoring country in the National Privacy Test, indicating that South Koreans may need to learn more about how to keep themselves safe online. Its total NPT score is 46% compared to 64% of Singapore.

Looking at privacy awareness, Japanese respondents scored the lowest among all 25 countries, tying with Italy. This finding shows a substantial knowledge gap and suggests people in Japan may need to educate themselves about online privacy risks.

Despite that, respondents in Japan outperformed other

continue on page 21

countries in some questions. They understand the importance of reading terms of service and what tools to use for digital privacy, coming second after the top-performing country, Singapore.

Global internet privacy awareness is decreasing

The global NPT score hit 61% this year, which shows the decrease in the world's online privacy and cybersecurity awareness compared to 2022 (64%) and 2021 (66%).

Among the key **global takeaways:**

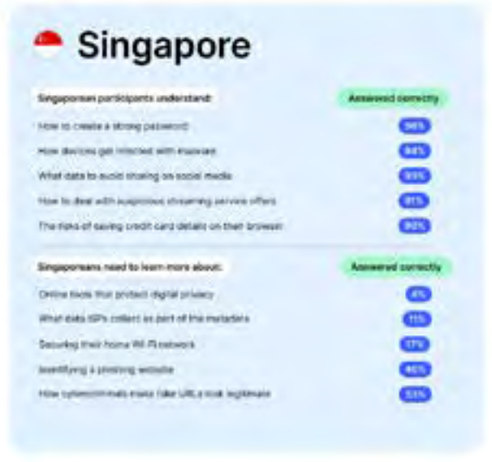
- People aged 30-54 have the best cybersecurity skills, with most Cyber Stars in this age group.
- Besides the IT sector, respondents from the finance and government industries got slightly higher NPT scores than others.
- People still underestimate the importance of reading terms of service. However, this metric is improving faster than others.

"I think there are a few reasons why cybersecurity knowledge is declining globally. The first and most important one might be the sheer volume of online activities and digital interactions that people engage in daily. Our previous research showed that Singaporeans spend more than 27 years of their lifetime online. Secondly, as technology continues to advance, cybercriminals also adapt their tactics, making it challenging for the average user to keep up. Also, there is a common misconception that cybersecurity is solely the responsibility of service providers," says Briedis.

Online security and privacy can be improved

To commemorate the approaching International VPN day (August 19), Briedis from NordVPN provides a list of steps people should follow in order to increase the privacy and safety of their online presence:

1. **Use strong and unique passwords.** Create strong passwords for each of your online accounts and avoid using the same password across multiple platforms.
2. **Use multi-factor authentication (MFA).** Implementing multi-factor authentication adds an extra layer of security by requiring users to provide additional verification, such as a one-time code sent to their phone, along with their password.
3. **Update your software regularly.** Keeping software, operating systems, and applications up to date is crucial for fixing known vulnerabilities. Regular updates ensure that security patches are applied promptly, reducing the risk of exploitation by cybercriminals.
4. **Always use a virtual private network (VPN).** A VPN encrypts your internet connection and helps protect your personal information from prying eyes. It is especially crucial when connecting to public Wi-Fi networks.
5. **Review and adjust privacy settings** on social media platforms, mobile apps, and other online services. Limiting access to personal data and choosing the minimum required permissions can help protect privacy.



Methodology: The National Privacy Test is an open-access survey, allowing anyone from around the world to take the test and compare their own results with the global ones. In 2023, 26,174 respondents from 175 countries answered 22 questions that evaluated their online privacy skills and knowledge. The 2023 data is analysed as of 07/19/2023 and presented in the report. If there is a difference with the webpage results, it means more people participated since July 19 and the result has slightly changed.

For more information, please visit nordvpn.com. ■

continue on page 22

CYBER VULNERABILITY EXPERT HACKUITY PREDICTS THE TOP FIVE CYBERSECURITY RED FLAGS IN APAC

- Hackuity, the award-winning risk-based vulnerability management provider, has released its latest predictions on the top cybersecurity trends in Asia Pacific (APAC) to look out for.
- APAC has been deemed the most attacked region in 2022 due to the rise of hybrid business environments and the increase of ransomware in the region, accounting for 31 per cent of all incidents worldwide.
- Data shows that 80 per cent of breaches still come from a lack of basic cybersecurity hygiene and only 15 per cent of organisations are considered cyber mature.
- Hackuity is recently recognised in the Grand Défi Stage 2 for its innovation strategy, an initiative launched by the French Government and financed through France 2030 by the European Union for its Great Cybersecurity Challenge.

Singapore – Hackuity, the award-winning risk-based vulnerability management provider, today shared its latest findings on current cyber threats, including the most critical red flags in Asia Pacific (APAC) and how businesses can defend against them. This comes amid a surge in cyber threats as attackers shift their focus to the region.

Image by Freepik

"Enterprises should double down on their cyber hygiene to ensure robust defence. At Hackuity, we observed that 80 per cent of breaches still come from a lack of basic cybersecurity hygiene and only 15 per cent of organisations are considered cyber mature, while more than half are still in beginner or formative stages. Most cyber threats can be prevented with steady investments, top-down willingness, and awareness of the risks. It is important for organisations to invest in not only people and processes but also the right technologies that can make a difference," said Pierre Samson, Chief Revenue Officer at Hackuity.

According to Hackuity, the main red flags are:

Advancements in Threat Intelligence and Response – Cyber threats are becoming more sophisticated, and organisations in APAC will likely need to invest in advanced threat intelligence capabilities to develop stronger incident response strategies. With more constrained resources and increasing workloads, companies will look to automate massively to keep pace with attackers. This includes utilising and leveraging automation, artificial intelligence (AI), and machine learning to detect and respond to threats more effectively.

Continuation of Cloud Security Challenges – Secure configuration and management of the cloud environment, including strong access controls, encryption, and protection of sensitive data, will continue to be a top priority as cloud adoption grows in APAC. Organisations will be seeking a single pane of glass to turbocharge their effectiveness and extract more value out of existing tools and investments.

Continued Shortage of Skilled Cybersecurity Professionals – What keeps CISOs awake at night? Demand for skilled cybersecurity professionals is expected to continue exceeding supply in APAC. Organisations need to invest in talent development and retention to bridge the skills gap and build a strong cybersecurity workforce, while exercising robust and intelligent cyber hygiene to automate tasks that go beyond human processing capabilities to rebalance practices and focus on people, processes, and technology.

Heightened Regulations – Governments play a key role in driving a holistic security approach across all sectors. In Southeast Asia, governments are rolling out a slew of data protection laws to secure critical governmental, organisational, and citizen data. For instance, Singapore recently changed its Personal Data Protection Act to tighten rules surrounding the misuse of data and mandatory reporting, while Thailand's legislation was updated in 2022 to mirror the European Union's General Data Protection Regulation measures more closely.

Ever-Increasing Attack Surface – Considering the decade-long spike of mobile and versatile digital usage across

continue on page 25

regions - resulting in social and professional media explosion - the number of possible touchpoints and attack vectors has increased. Hackers have revelled in this increase, as it has given them many more avenues to experiment with, more access to consumer data and a heightened ability to mine private and valuable data.

APAC retained the top spot as the most attacked region in 2022, accounting for 31 per cent of all incidents worldwide, according to IBM's Security X-Force Threat Intelligence Index. The embrace of a hybrid business environment during the pandemic increasingly exposed IT systems to exploits by hackers using automation and artificial intelligence (AI) to enhance the frequency of attacks. The study showed that malware, which provides access to compromised systems, is used in 20 per cent of all cases.

Samson added, "The future of cybersecurity in APAC lies in continuous adaptation, the adoption of cutting-edge technologies, and the establishment of collaborative efforts between public and private sectors. Only by embracing these challenges and addressing emerging threats, the region can fortify their cybersecurity resilience through robust strategies and adaptive measures."

Already the winner of multiple prestigious awards in Europe, Hackuity's deep-tech innovation strategy has recently been crowned by the Grand Défi Cyber Stage 2 – an initiative launched by the French Government and financed through France 2030 by the European Union for its Great Cybersecurity Challenge. Hackuity, along with its partners, is proud to be one of the five winners of the Grand Défi Stage 2 and to contribute to the development of the French cyber ecosystem worldwide.

Moving ahead, Hackuity is capitalising on the competitive advantages offered by the Attack Path Monitoring project's disruptive innovations. The company's ambition is to generate over 50 per cent of revenue internationally by the end of 2024, and position Hackuity as a leader in the global Attack Surface Management market.

For more information, please email sales@tdsi.co.uk or visit www.hackuity.io. ■

SOPHOS AGAIN NAMED CUSTOMERS' CHOICE FOR ENDPOINT PROTECTION PLATFORMS (EPP) IN THE GARTNER® PEER INSIGHTS™ VOICE OF THE CUSTOMER REPORT

Only Vendor Recognized as Customers' Choice Across EPP, Managed Detection and Response (MDR), Network Firewalls, and Mobile Threat Defense

Singapore – Sophos, a global leader in innovating and delivering cybersecurity as a service, today announced it has once again been named a Customers' Choice in the Gartner® Peer Insights™ Voice of the Customer for Endpoint Protection Platforms (EPP) report. Sophos is the only vendor recognized as a Customer's Choice across EPP, managed detection and response (MDR), network firewalls, and mobile threat defence.

Image by Freepik

Reflecting the breadth of Sophos' endpoint market coverage, Sophos is the only vendor to be named a Customers' Choice across all industry segments evaluated in the new EPP report – including Education, Finance, Healthcare, Manufacturing, and Services – with an overall customer rating of 4.8 out of 5 across 451 verified customer reviews as of June 2023. Furthermore, Sophos is also the only vendor to be named Customers' Choice for the entire Education market category.

"Superior endpoint protection that works for you and with you is crucial for shielding against today's innovative adversaries, who our research shows are actively

exploiting security weaknesses such as unpatched vulnerabilities and compromised credentials to bypass traditional defences," said Raja Patel, senior vice president of products and managed services at Sophos. "Relentless innovation is at the heart of everything we do at Sophos, and this repeated customer recognition is validation that the multi-layered protections in Sophos Intercept X – from adaptive defences that automatically respond to an attack to the most comprehensive anti-exploit capabilities on the market – are delivering superior security outcomes in the real-world."

Select Sophos Intercept X customer quotes from the report include:

"Sophos Intercept X provides incredible performance with ease of use of security: Intercept X provides clear visibility of evils inside the network and protects from virus/ malware/cyber threats with a prompt response and attractive statistical reports," said an infrastructure manager in the education industry

"This product is the best endpoint product out there: The overall experience has been excellent. Sophos intercept X has been a phenomenal product and the way it detects and neutralises the risk before it can cause any harm to our organisation is really commendable," said an IT manager in the education industry

"Best endpoint protection from Sophos: We [have been] using Sophos Intercept X for more than five years now... it has successfully secured our organisation from at least four major incidents," according to a senior IT administrator in the IT services industry

"Sophos offers rock solid protection at worth value, (and I) love to recommend Sophos (to) everyone: (Intercept X) is hands down the best zero-day threat endpoint protection I have used to date in terms of effectiveness," said a technical support leader in the healthcare and biotech industry

Sophos Intercept X protects more than 300,000 organisations against advanced attacks, offering multiple layers of security for unparalleled protection against known and unknown malware and exploits. Introduced this year, Sophos' industry-first Adaptive Attack Protection capability provides an automated step-up in endpoint security. Adaptive Attack Protection immediately activates heightened defences when a hands-on-keyboard attack is detected. The unique capability dynamically adjusts protections based on threat context to stop in-progress attacks and provide defenders with valuable additional time to respond.

Sophos Intercept X is part of the Sophos Adaptive Cybersecurity Ecosystem, which integrates Sophos' portfolio of products, services and Sophos X-Ops threat intelligence for faster and more contextual and synchronised detection, protection and response. It is easily managed in the cloud-native Sophos Central platform alongside other solutions, where users can oversee installations.

Already this year, Sophos was named a Leader in the 2022 Gartner® Magic Quadrant™ for Endpoint Protection Platforms (EPP) for the 13th consecutive time.

A complimentary copy of the Gartner Peer Insights Voice of the Customer: Endpoint Protection Platforms report is available at https://www.gartner.com/doc/reprints?id=1-2F1ML1JT&ct=230919&st=sb.

For more information, please visit www.sophos.com.■

ROHDE & SCHWARZ AND FRAPORT EVALUATE THE WORLD'S FIRST WALK-THROUGH SCANNER FOR PASSENGERS

Fraport began testing the world's first walk-through security scanner for passengers at Frankfurt Airport. The R&S QPS Walk2000 from Rohde & Schwarz is designed to speed up security checks. The first of these scanners is currently in use in Concourse A of Terminal 1. Passengers simply walk through the scanner at a normal pace without stopping. The test and evaluation phase is set to last up to six months and will provide Fraport and Rohde & Schwarz with important information to help optimise the system.

Munich, Frankfurt – The R&S QPS Walk2000 is a 360° walk-through scanner that can detect all kinds of items quickly and contact-free. The scanner provides a more pleasant security experience: passengers do not have to stop to be scanned and can instead slowly walk through the R&S QPS Walk2000. The millimeter wave technology can also penetrate multiple layers of clothing, making it unnecessary to remove jackets and coats, for example. This makes a big difference in terms of comfort and personal privacy when going through security.

AI based detection software automatically identifies metallic and non-metallic objects. Any anomalies detected on passengers are accurately displayed in real time on a unisex avatar, reducing the need for follow-up checks. If, however, a check is needed, security staff can focus on the areas that have triggered an alarm instead of patting down the passenger.

The joint evaluation of the walk-through scanner at Frankfurt Airport by the German Federal Police and Fraport is yet another example of the continued excellent collaboration between Fraport and Rohde & Schwarz since Fraport assumed management of the airport's security checks. Fraport acquired and set up the R&S QPS Walk2000, but it is the German Federal Police who are responsible for all security-related tests and will ultimately grant approval for use in day-to-day operations. The aim of the walk-through scanner is to make security checks faster and more comfortable for passengers while maintaining the same high level of security. The checkpoints selected for the test phase are in the Schengen Concourse A of Terminal This concourse is ideal for such a test due to its high foot traffic: on average, 15,000 passengers use this concourse every day.


The R&S QPS Walk2000 is the world's first walk-through scanner being used to check passengers at an airport.

The test phase at Frankfurt Airport aims to provide a direct comparison of the R&S QPS Walk2000 and the tried and tested R&S QPS201 scanners already installed and reveal any immediate differences. The collaborative trial installation aims to make walk-through security checks for passengers just as reliable as the highly efficient checks provided by the R&S QPS201.

For more information, please visit www.rohde-schwarz.com. ■

SHA ZHU PAN SCAMMERS USE FAKE CRYPTOCURRENCY TRADING POOLS TO STEAL MORE THAN $1 MILLION, SOPHOS REPORTS

Sophos Details the Story of One Scammed Victim in the Trading Pool Who Lost $22,000 in One Week.

Singapore – Sophos, a global leader in innovating and delivering cybersecurity as a service, today released findings on a major sha zhu pan (pig butchering) operation utilising fake trading pools of cryptocurrency (liquidity pools) to steal more than $1 million. The report, "Latest Evolution of 'Pig Butchering' Scam Lures Victim in Fake Mining Scheme," details the story of one of the scammed victims in the pools, named *Frank, and how he lost $22,000 in one week after "someone" pretending to be "Vivian" on the dating app MeetMe contacted him. After Sophos X-Ops investigated Frank's story, the team uncovered a total of 14 domains associated with the scam

operation, as well as dozens of nearly identical fraud sites that, together, netted this one "ring" of pig butcherers more than $1 million in three months.

This scam takes advantage of the largely unregulated world of decentralised finance (DeFI) cryptocurrency trading applications. Such applications create "liquidity pools" of various types of cryptocurrencies that users can then access to make trades from one cryptocurrency to another. Those who participate in the pool receive a percentage of any fee paid when a trade is made, creating an enticing return on investment. To join a pool, participants first have to sign an online smart contract—a contract that gives another account (typically the operators of the pool) permission to access participants' wallets to facilitate trades. Fake pools, which pig butcherers are increasingly utilising to syphon funds from targets, operate in much the same way. However, unlike legitimate pools, at some point these scammers "pull the rug" and empty the entire liquidity pool for themselves.

"When we first discovered these fake liquidity pools, it was rather primitive and still developing. Now, we're seeing sha zhu pan scammers taking this particular brand of cryptocurrency fraud and seamlessly integrating it into their existing set of tactics, such as luring targets over dating apps. Very few understand how legitimate cryptocurrency trading works, so it's easy for these scammers to con their targets. There are even toolkits now for this sort of scam, making it simple for different pig butchering operations to add this type of crypto fraud to their arsenal. While last year Sophos tracked dozens of these fraudulent 'liquidity pool' sites, now we're seeing more than 500," said Sean Gallagher, principal threat researcher, Sophos.

Sophos X-Ops first learned of this liquidity mining operation from a victim named Frank. Frank had connected on the dating app MeetMe with a scammer hiding behind the persona of Vivian, a German woman supposedly living in Washington, D.C. for work. For weeks, Frank chatted with Vivian, who mixed her romantic promises with persistent attempts to convince Frank to invest in crypto.

Eventually, Frank opened a Trust Wallet account (a legitimate app for converting dollars to cryptocurrency) and connected to the link to the liquidity pool site Vivian recommended. In reality, the pool site was a fraud site utilising the brand of Allnodes, an established decentralised finance platform provider, as a cover. Between May 31 and June 5, Frank invested $22,000 in the scheme. Just three days later, the scammers emptied Frank's digital wallet. Frank, looking to recover his money, turned to Vivan, who claimed he needed to invest even more in the pool to recover his funds and reap the "rewards." While waiting for his bank to authorise a money transfer to Coinbase, Frank started researching what was going on and came across an article on liquidity mining from Sophos. At this point, Frank reached out to Gallagher for help.

Even after Gallagher instructed Frank to block Vivian, she eventually found him on Telegram and continued her attempts to entice him into "continuing their investment," going so far as to send a lengthy, emotional letter that was very likely created by a generative AI app.

"What makes these sorts of scams particularly tricky is that they don't require any malware to be installed on a victim's device. They don't even involve a fake app, like some of those we've encountered in other CryptoRom scams. This entire fake liquidity pool was run through the legitimate Trust Wallet app. At one point, Frank even tried to contact Trust Wallet's support to recover his money, but he connected with a fake support contact from the fraudulent liquidity pool site. There is no regulation of these pools, legitimate or otherwise, on these crypto apps. These scams succeed solely through social engineering, and the scammers are persistent. Vivian continued trying to contact Frank for weeks after he blocked her on WhatsApp.

"The only way to stay safe from these scams is to be vigilant and know that they exist and how they operate. That is why Frank wanted to share his story. Users need be wary of anyone they have no connection with reaching out to them suddenly via any dating app or social media platform, particularly if the 'person' reaching out wants to move the conversation to a platform like WhatsApp and then discusses investing in cryptocurrency," said Gallagher. Sophos has shared its data on this case with Chainalysis and Coinbase, as well as other threat intelligence professionals in the cryptocurrency space, all of whom continue to investigate. People who believe they may be a victim of pig butchering or liquidity mining fraud are free to reach out to Sophos. They should also reach out to their local law enforcement for assistance.

For more about the rise of liquidity mining scams in "Latest Evolution of 'Pig Butchering' Scam Lures Victim in Fake Mining Scheme," go to Sophos.com. ■

TRUE DIGITAL GROUP PARTNERS WITH VECTRA AI TO DELIVER MACHINE LEARNING CAPABILITIES FOR IMPROVED RISK MANAGEMENT

Leading Thai digital transformation enabler utilises Vectra AI's Attack Signal Intelligence to reduce false positives for better risk prioritisation

Singapore – Vectra AI, the leader in AI-driven cyber threat detection and response for hybrid and multi-cloud enterprises, has been appointed by True Digital Group (True), Thailand's leading digital transformation enabler, to strengthen its defence against a landscape of growing cyber threats.


Image by Freepik

Today's security teams are tasked with protecting progressively sophisticated, fast-paced cyberattacks. Yet, the ever-expanding attack surface combined with evolving and evasive attacker methods and increasing security analysts' workload results in a vicious "spiral of more" that is preventing security teams from effectively securing their organisation.

True has selected Vectra AI and its Attack Signal Intelligence™(ASI) technology to optimise the organisation's ability to detect and prioritise threats, specifically to automatically filter and reduce high levels of false positive alerts via machine learning and allowing its security team to only focus on critical incidents.

Tithirat Siripattanalert, Group CISO and CDO at True comments, "Organisations in Thailand have been bearing the brunt of cyberattacks. The persistence of these threats highlights the ongoing need for True to remain ever vigilant and heighten our cyber risk management posture. Previously, we found the overwhelming amount of false positive alerts particularly problematic as they took up additional time for our SOC team to investigate.


Image by Freepik

"With the deployment of Vectra AI, we can now identify suspicious activities in real-time which the previous traditional technology wasn't able to. Vectra Attack Signal Intelligence helped us prioritise the most urgent alerts with its machine learning technology which rapidly analyse abnormal behaviour. This significantly reduced the volume of false positive alerts and gave our security team the ability to focus on critical incidents and remediate threats more effectively," said Siripattanalert.

David Sajoto, Regional Vice President of Asia Pacific and Japan at Vectra AI said, "As enterprises shift to hybrid and multi-cloud environments, SOC teams are continuously finding themselves victims to more and increasingly unsustainable attacks. According to Vectra research, 8 out of 10 (83%) feel outgunned against modern attacks, with 63% of SOC analysts saying their attack surface has significantly increased in the past three years. Additionally, research showed that security analysts are unable to deal with 67% of the daily alerts received with 83% reporting that alerts are false positives and not worth their time.

"We are delighted to be working with True Digital Group in Thailand to strengthen their security resilience by providing greater clarity on their most urgent threats. Our Vectra ASI platform is already delivering targeted visibility across True's network, reducing the noise and improving operational efficiencies. We look forward to extending the relationship further to support their corporate customers," Sajoto said.

For more information, please visit www.vectra.ai. ■

ALKIRA BOOSTS GLOBAL EXPANSION EFFORTS FOR ENTERPRISES WITH CLOUD EXCHANGE POINT PRESENCE IN CHINA

With Alkira, companies can finally centralise networking in China with robust segmentation and a uniform policy.

San Jose, CA – Alkira, the pioneer in agentless, multi-cloud networking, today announced the availability of Alkira Cloud Exchange Point (CXP) in China, extending Cloud Network-as-a-Service in the country for seamless global network connectivity. With Alkira CXP presence in China, enterprises can simplify deployment and operations by leveraging a unified management and control plane for China and the rest of the world. Alkira CXP is delivered entirely a service, meaning no hardware, software, or agents need to be installed.


Image by Freepik

Working with its trusted partner, CBC Tech, a fully licensed, next-generation Network-as-a-Service (NaaS) provider, Alkira delivers a fully compliant turnkey solution for China connectivity. CBC Tech, renowned for its comprehensive offerings, delivers CBC NaaS—an umbrella of next-generation networking solutions, including SD-WAN, SASE and Cloud Networking, designed to empower global enterprises operating in China. CBC NaaS accelerates time-to-market while ensuring business continuity and security.

"As a leader in navigating the complexities of China's tech environment, we are excited to collaborate with Alkira to extend their cloud networking capabilities to China," stated Shu Yee, Hoo, Vice President (Products and Solutions) at CBC Tech. "Our joint efforts will empower businesses to access cutting-edge networking solutions that drive efficiency, compliance, and security, ensuring a strong foundation for digital transformation in the region."

The Alkira CXPs are virtualized points of presence that leverage the hyperscale infrastructure of the public cloud. With a presence in China, enterprises can direct the entire NaaS without the complexity of deploying and managing separate domains of infrastructure for China regions. A user-friendly interface allows you to easily exchange routes between global networks and China, giving operators a single interaction surface for routing, traffic control, enhanced visibility, and intent-based policy.

"China is a critical business hub and enterprises typically struggle with fast, reliable connectivity to the country due to the network regulations that require a significant investment of time, effort, and money" said Atif Khan, Chief Technology Officer at Alkira. "Working with CBC Tech adds a wealth of expertise and a deep understanding of China's cloud and networking landscape to our offering. Alkira is committed to delivering an experience that maximises speed, simplicity, and scalability while ensuring enterprise-grade security for our customers, so we knew this was an area we wanted to address. From Intra-Cloud connectivity to Inter-Cloud connectivity to the rest of your global network, Alkira's CXP presence in China provides the world's most seamless experience with unmatched performance, capabilities, and integrations."

Hybrid Cloud is Growing in China

In Gartner's Market Guide for Cloud Infrastructure and Platform Services, China notes that by 2025, adoption of hybrid cloud will increase to more than 70% of large organisations in China (up from less than 40% in 2021).

However, with limited cloud options and data sovereignty issues in China to grapple with today, American businesses have been forced, in many instances, to build their own architectures or leverage a colocation data centre to do business in China. Going this route, enterprises cannot segment data from the rest of their network, which adds more complexity for IT and security leaders who are already strapped for time with shrinking staffs and budgets. Furthermore, trying to manage this process on their own makes them more vulnerable to cyberattacks, doesn't allow them to have end-to-end visibility of their networks, and requires a considerable amount of time and money.

Alkira Makes it Easy to Connect to China

With Alkira, enterprises can centralise networking in China, with access to robust segmentation and a uniform policy. As opposed to other cloud providers in China that want you to use their services only, Alkira is focused on speed, simplicity, scalability, and security, regardless of the services that are deployed. As one of the only multi-cloud platforms that has a cloud backbone as a service, Alkira empowers enterprises to easily stitch one network together, including China, allowing them to spot and eliminate redundancies and cut costs. Key benefits include:

- Unified Global Networking – Alkira's as-a-service platform provides an identical experience for China and all other Alkira regions worldwide.
- Network Services – Enhance capabilities and operations by streamlining the deployment and management of network and security services available in the Alkira Marketplace.
- 100% as a Service - No hardware to buy, no software to licence, no virtual agents to manage. Alkira delivers the industry's leading global connectivity with turnkey business outcomes, on-demand resources, and flexible consumption.

Learn more about Alkira's CXP presence in China here: https://www.alkira.com/blog/china-cxp-availability-global-backbone-without-borders/ ■

THE SIMPLE TOUCH OF A FINGER TO ADDRESS REAL-WORLD SECURITY AND ACCESS CHALLENGES

By Vito Fabbrizio

Fingerprint technology is a mature, proven method for user authentication across a range of industries, use cases and environments.

Selecting the right fingerprint technology often comes down to the level of security and match accuracy required, the capabilities and features needed, and the usability to achieve both adoption and productivity.

Why fingerprints

The fingerprint is one of the most widely used methods for biometric authentication due to its speed, ease of use, high level of accuracy and cost-effective nature.

Fingerprints possess several unique features that make them valuable for various applications.

Firstly, they are universal, meaning almost everyone has them. Secondly, each person's fingerprint is unique and distinguishable, making it an excellent identifier. Additionally, fingerprints are reasonably stable and permanent, remaining consistent over time. They are also easily collectible, as they can be acquired, measured and processed with ease.

Moreover, fingerprints are defendable, meaning they can be protected from abuse, misuse, theft, imitation and substitution. When combined with recognition techniques, fingerprints are highly performant, offering accuracy, speed,


Image by Freepik

scalability and ease of use across various applications. They are also adoptable, with the highest adoption rate for biometric authentication, according to an industry report.

The three elements of fingerprint biometric systems

A fingerprint biometric system consists of several components which work together to make an effective solution.

The process begins with the fingerprint sensor, specifically designed for the capture and preliminary processing of fingerprint data. Subsequently, a biometric algorithm is employed to extract minutiae data from the fingerprint, which includes details like ridge endings, ridge bifurcations,

ridge islands, minutiae orientation, and various measurements.

Additionally, a presentation attack detection (PAD) technique may be implemented during the fingerprint capture to verify the authenticity of the fingerprint, ensuring that it originates from a living person.

If the predetermined conditions are satisfied, the digital fingerprint dataset is then securely stored as a record known as a template within a cryptographically protected storage enclave.

When a matching operation is required, the presented fingerprint undergoes a re-evaluation for liveness, and the corresponding template is retrieved from the secure storage for the matching process to take place.

The following are three important factors to consider when identifying an optimal biometric authentication system from a low-performing one:

How well the capture works for a range of fingers, skin types and print conditions across different environmental conditions such as temperature, humidity, light, surface oils, dust and dirt,

How effective PAD works to identify and reject fake finger attempts, and How well the system can accurately match legitimate users while rejecting illegitimate users.

Key considerations for selecting the right fingerprint technology

The key considerations and requirements for selecting fingerprint technology boil down to a balance between the total cost of ownership, security, suitability and usability.

Security:

- Is the industry highly regulated such as financial services, healthcare, government entities or law enforcement?

The Three Elements of Fingerprint Biometric Systems

- Are advanced capturing and biometric authentication specifications mandatory?
- Is there a need to ensure anti-spoofing?
- Is there a need to have endpoint security so networks, systems and data behind the firewall won't be impacted in the case of the fingerprint device being hacked?

Suitability:

- Will the technology be embedded in devices that require low power, battery operated capability and portability?
- Will the technology need to fit into small spaces or be used in difficult elements or environments, indoor or outdoor?
- Is durability from unpredictable weather and lighting conditions a factor?
- What applications will the technology be used for, such as mission-critical border control or more common commercial use?

Usability

- Does the technology perform capture and matching with ease and consistency?
- Does the technology need to handle high volumes of fingerprint captures and matches?
- Is matching quick and accurate to enable user productivity instead of friction frustration?
- Will the device be used by multiple people in a shared workstation setting?
- Can the reader handle all types of fingerprints and diversified demographics for the mass population?

Based on the above criteria, organisations can decide what kind of fingerprint capture technology best fits their deployment.

For example, for a shared environment with limited space, such as healthcare clinician's terminals, a slim and durable capacitive sensor would be a good fit. For more demanding use cases in highly-regulated, mission-critical environments that can't risk an identity misstep, such as banking or border crossing, organisations should consider more advanced technologies such as multispectral imaging (MSI) readers.

With the simple touch of a finger, biometrics empower a wide range of use cases across multiple industry sectors ranging from banking and finance, retail, and healthcare, to government and law enforcement.

As industries evolve their identity and access strategies, they face unprecedented threats and challenges from fraud, account takeover and impersonation. Fingerprint biometrics continue to offer the most accurate, efficient and secure solution that addresses real-world challenges faced by enterprises today. ■

SMITHS DETECTION ADVANCES OPEN ARCHITECTURE INITIATIVE WITH NEURAL GUARD

Smiths Detection, a global leader in threat detection and screening software, announced that they will be collaborating with Neural Guard, a provider of artificial intelligence-based automatic detection algorithms, to integrate their threat recognition software with Smiths Detection's HI-SCAN 6040 2-is X-ray scanner using the common API (Application Programming Interface) developed by EOS (the European Organisation for Security).

The HI-SCAN 6040 2-is is used in airports and building entrances around the globe to screen bags and other personal items for concealed threats and contraband. Integration with advanced threat detection software such as Smiths Detection's iCMORE weapons or Neural Guard's EyeFox can speed up the screening process by automatically alerting operators to knives, guns, bullets and other threats.

The collaboration is part of Smiths Detection's ongoing Ada Initiative that is accelerating the adoption of open architecture into the security environment.

Cymoril Metivier, Global Director of Digital at Smiths Detection, said: "Automatic threat detection algorithms will transform security screening by making it more accurate and more efficient. Open architecture is an enabler of this by linking together existing infrastructure with software, sensors and algorithms from a choice of suppliers into one integrated system."

Moshe Cohen, Chairman of Neural Guard, said: "We're delighted to be working with Smiths Detection as they advance the progress of open architecture into the security screening environment. By working together, we're able to provide their customers with great choice as they seek to upgrade their systems." ■

VEEAM ANNOUNCES BENI SIA AS THE NEW GENERAL MANAGER AND SENIOR VICE PRESIDENT, APJ

Singapore – Veeam® Software, the leader in Data Protection and Ransomware Recovery, has announced it has appointed Beni Sia as the new General Manager and Senior Vice President of Asia Pacific and Japan (APJ), responsible for Veeam's business operations and growth across the region.

Sia brings more than 20 years of experience in the IT industry to the role, primarily in working with customers and partners across the APJ region to drive business growth and transformation. Most recently, he served as Vice President of Southeast Asia and Korea at Veeam and led growth and expansion across 12 markets.

"Addressing the rising threat of cyber-attacks is a top priority for every organisation with 82% of organisations in APJ hit by ransomware. Given the rapid adoption of new technology, data protection and ransomware recovery is critical," said Sia. "Veeam's success is based on combining our customer focus with our commitment to our channel and alliance partners. I am excited about the incredible opportunity we have to help customers across Asia keep their businesses running."

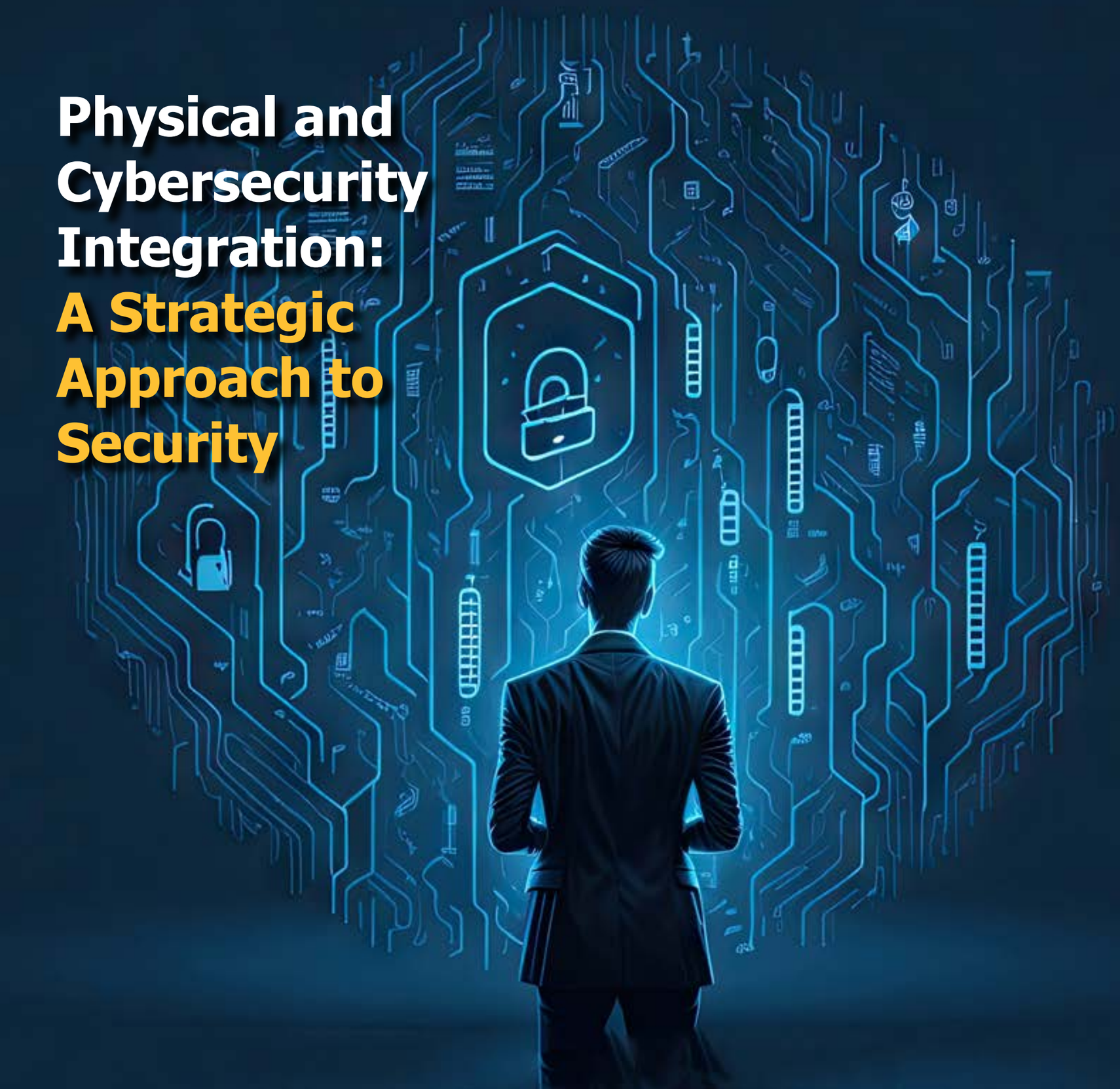
In his new role at Veeam, Sia will spearhead the company's growth strategy for the entire APJ region.

"Beni is an accomplished business leader who, over the past three years, has demonstrated his ability to build and lead high-performing teams while delivering outstanding customer outcomes," said John Jester, Chief Revenue Officer (CRO) at Veeam. "His appointment is a great testament to our commitment at Veeam to develop and recognize great talent across the company. I'm excited to support him as he leads our continued growth and momentum across the APJ region with customers, partners and alliances."

Veeam delivers consistent, double-digit revenue growth year-over-year (YoY) and was recently ranked as the #1 global provider of Data Replication and protection software in 2022H2 by the latest International Data Corporation (IDC) Semiannual Software Tracker. Veeam had the fastest YoY growth rate in 2H22 among the top five D&P vendors at 8.1% and outperformed the global market average. In the Asia Pacific & Japan (APJ) region, Veeam recorded a 20.7% YoY growth, the highest among the top five vendors.

For more information, please visit www.veeam.com. ■

Physical and Cybersecurity Integration: A Strategic Approach to Security



Each day, any business organisation comes across digital and physical security threats. The reliance of work on technology has increased the risk of unauthorised access and affecting business. About 88% of boards agree that cybersecurity is a risk to business and that it's more than an IT problem to fix.

In addition, physical security is also at risk as it is closely connected with cybersecurity. An attack on either of these two can impair the other. One cannot be given more importance than the other as they combine to form a tight, secure system.

The growing infrastructure of any organisation relies on physical as well as cybersecurity to function without any operational hiccups. Therefore, it needs utmost security, and separating the two may lead to gaps and be a major business risk.

We'll cover why physical and cybersecurity integration is a smart and effective choice for protecting business assets.

Understanding Physical and Cybersecurity

Physical security of an organisation refers to protecting physical assets such as property, people, buildings, machinery, and information. Installing access controls, intrusion detection alarms and surveillance along with security personnel is one way to attain physical security.

With ample security in place, an organisation may prevent theft, damage or unauthorised access. These features can alert the security guards to take action and prevent further damage.

The alerts may be sent online or through internal communication systems. This is where cybersecurity comes in. Cybersecurity is all about protecting digital assets, networks, and data applications. Any breach in computer security may impair an organisation's physical and cyber access.

Measures such as secure firewalls, intrusion detection systems, and antivirus may contribute to stronger cybersecurity. Overall, a multi-level approach is necessary as attackers try to disrupt the systems with advanced tactics such as malware, ransomware, and phishing attacks.

Keep on reading to learn how both physical and cybersecurity combine to secure an organisation from all kinds of attacks.

Need for Integrating Physical and Cybersecurity

Are you still wondering what the need is for integrating physical and cybersecurity? By merging both, the organisation can create an attack-proof system. Approaching physical and cyber security as a combined force can deter threats, attacks and unauthorised access.

This need arises due to the fact that the attacks are more hybrid these days. The attacker plans to disrupt both physical and cyber assets. Anyone who has access to physical assets may damage the server room or computer systems. This physical attack will impact online security.

Similarly, an attack on the online communication system may not allow the security personnel to contact each other. The attacker may manipulate the company staff with wrong online data and communication.

Here are some more examples to show the impact of physical and cyber security gaps:

- Unauthorised access to hardware and retrieval of sensitive data via USB
- Adding virus to the hardware
- Introducing malware in the internal organisation network
- Cyber-attack on hospital systems and medical devices
- Virtually shut down of machinery, HVAC system, and security doors
- Impairing communication, online video surveillance, and data sharing
- Barring online emergency response or overriding command systems
- Wireless hacking of systems

Recently, banks, organisations and even hospitals have suffered due to cyber attacks. This shows how physical and cybersecurity are connected and we cannot isolate them. Any negligence in the integration can put the business at a high breach risk.

Therefore, the present need is to combine Internet of Things(IoT) with Industrial Internet of Things(IIoT) devices for higher security. Only a resilient system with physical and cybersecurity can survive numerous attack attempts.

Are there any current challenges to integration?

Some organisation may go through the following challenges during the integration

- Technological barriers due to lack of knowledge and training
- Limitations due to compliance and regulations
- Lack of collaboration throughout the enterprise
- Limited funds to integrate ample security measures
- No coordination between departments
- Delayed identification of security risks
- Disagreements between departments
- Mismanagement and improper response planning
- Inadequate risk assessment

Significant Benefits of Integrating Physical and Cybersecurity

The goal of security is to assess risks and bridge the departmental and management gaps. Below are significant benefits of physical and cybersecurity integration.

Enhance security

Since physical and cybersecurity are connected, integrating the two will make the organisation ready to fight any type of attack. With a planned response system and robust security structure, the threat will be nipped in the bud. Several options, such as secure access controls, firewalls and surveillance systems, can be added to enhance security.

Cost savings

The integration may sound like a costly ordeal; however, having a single reliable network for physical and cybersecurity can save money. The two will not have to be assessed and maintained separately, hence saving on individual expenditure.

Reliable right management

Assessment of physical and cyber security together may help in understanding the security risks. This will lead to a timely resolution and prevent the threat from doing any damage to the system.

Regulatory compliance

Certain regulations have made it mandatory to be prepared for physical as well as cyber-attacks. Following the regulations closely will help in achieving a regulatory-compliant status. In addition, it will give a framework for better security for all.

Ways to Strategically Integrate Physical and Cybersecurity

As discussed above, physical security and cybersecurity go hand in hand. Ignoring either of them may prove to be a massive mistake, leading to financial and operational losses. Needless to say, the ultimate goal is to be equipped with ways to handle modern threats with minimal damage.

Integrating security can predict threats and prevent cyber attacks that also pose a threat to physical assets and vice versa. Here is how physical and cybersecurity integration may be done.

Preliminary preparation

Various departments have to come together to integrate physical and cyber security successfully. The key to uninterrupted data sharing and risk assessment is communication and collaboration. The preliminary assessment should comprise a proper security framework. There should be a focus on transparent communication among the departments in an organisation.

The coordination of roles and responsibilities should follow it. Overall, there should be strategic and fruitful collaboration between the management. The departments may collaborate to prioritise crucial things and assign tasks to better security as per the skills.

Securing the building and property

Physical security involves prohibiting access to hardware, equipment and IT systems. Adding RFID security card systems, smart cards and biometric fingerprint locks may help in securing the property. Giving limited access to certain departments or new employees is another way to enhance physical asset security. Add access points with multiple identity verifications to access the building and systems. A reliable alarm system to detect any breaches can also be installed for timely alerts.

Network security

Having a multi-factor authentication to enhance internal network security is a good idea to protect physical assets. The multi-level authentication works well as anyone will require certain physical key cards or codes to access the network system. Therefore, an intruder will fail to access the network when attempting

The goal of security is to assess risks and bridge the departmental and management gaps. Below are significant benefits of physical and cybersecurity integration.

continue on page 36

Images by Freepik

a single system breach. Additionally, this failed access will alert the organisation to keep its guard up.

Protecting human resource

An organisation cannot work without its human force. Protecting those who work in the company is necessary to maintain trust and productivity. This may include the provision of physical security, surveillance cameras, identity protection and management of healthcare or financial information.

Securing the data

We cannot emphasise enough the importance of securing the data. Apart from data security, there should be protocols in place to move data from one location to another.

Images by Freepik

Additionally, the data should be protected in a high-security system with restricted access. Centralising the data in a single safe location may keep it safe from online attacks and physical malware attacks.

Employee training

As your business switches to integrated security, all the employees may benefit from training and orientation. They must be made aware of physical and cybersecurity integration and its importance. This way, they can contribute and be cautious in compromised situations. Regular seminars and classes may be conducted with refresher courses and plans to respond to security threats.

Monitor online activity

Keeping a close on network traffic and information sharing can prove to be a useful tool. Make sure your company uses firewalls and detection alerts to learn about new threats. Any unusual activity should not be ignored and analysed carefully.

Response planning

Proper response planning ensures all the departments are ready for threats. Even with the best measures in place, the organisation should prepare beforehand. The response plan may also include revoking restricted area badges and cards in case of lost/stolen ones. Regular testing of these response plans can help in reducing response time.

Automatic shutdown of online systems in case of malware and access prohibition for unauthorised access may be significant in preventing damages. These protocols can be in place until the threat is resolved.

Regular audit

Auditing the access log and data history helps in the management of digital assets. This way, any discrepancy in the data can be detected and assessed as a threat and dealt with accordingly. An audit team must be set up to keep a check on logs and maintain additional data with anytime access.

Keeping a close on network traffic and information sharing can prove to be a useful tool. Make sure your company uses firewalls and detection alerts to learn about new threats. Any unusual activity should not be ignored and analysed carefully.

Wrapping Up

To summarise, physical and cybersecurity are critical components of an organisation. They have to be integrated to protect the assets from operational threats and unauthorised use. Integration of both ensures the physical assets are protected while online assets remain in the organisation's control.

These security measures not only protect from outside threats but also discourage any misuse by a new/malicious force inside the company. Dealing with security threats is an effective way to reduce threats and asset risk exposure. Regular risk assessment, security protocol audits and ample modern security integration can strengthen the organisation to keep functioning optimally. ■

COMING SOON

OCT 25 – 28 2023
China Public Security Expo 2023
Shenzhen, China
https://cpse.com

NOV 1 – 3 2023
Secutech Thailand 2023
Bangkok, Thailand
https://secutechthailand.tw.messefrankfurt.com

NOV 14 – 16 2023
ISC East 2023
New York, USA
https://www.discoverisc.com

DEC 7 – 9 2023
IFSEC India 2023
New Delhi, India
https://ifsecindia.com/

JAN 16 – 18 2024
Intersec 2024
Dubai, UAE
https://intersec.ae.messefrankfurt.com

APR 9 – 12 2024
ISC West 2024
Las Vegas, USA
https://www.security-essen.de

SEP 17 – 20 2024
Security Essen 2024
Essen, Germany
https://secutechvietnam.tw.messefrankfurt.com

SUBSCRIPTION FORM

Email your order to:
yvonne.ooi@tradelinkmedia.com.sg

PRINT

Please (√) tick in the boxes.

☐ **Southeast Asia Building**
Since 1974

☐ **Southeast Asia Construction**
Since 1994

***1 year** (6 issues) per magazine*

Singapore	○ SGD$70.00
Malaysia / Brunei	○ SGD$120.00
Asia	○ SGD$180.00
America, Europe	○ SGD$220.00
Japan, Australia, New Zealand	○ SGD$220.00
Middle East	○ SGD$220.00

DIGITAL

Bathroom + Kitchen Today
Since 2001

Bathroom + Kitchen Today
is available on digital platform.

http://bkt.tradelinkmedia.biz

Lighting Today
Since 2002

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

http://lt.tradelinkmedia.biz

Security Solutions Today
Since 1992

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

http://sst.tradelinkmedia.biz

Personal Particulars

Name:
Position:
Company:
Address:
Tel: **E-Mail:**

IMPORTANT
Please commence my subscription in _____ (month/year)

Professionals (choose one):

☐ Architect ☐ Landscape Architect ☐ Interior Designer ☐ Developer/Owner
☐ Property Manager ☐ Manufacturer/Supplier ☐ Engineer ☐ Others

☐ Bank transfer payable to:
Trade Link Media Pte Ltd

Bank Details

Account Name:	Trade Link Media Pte Ltd
Account Number:	033-016888-8
Name of Beneficiary Bank:	DBS Bank
Address of Beneficiary Bank:	12 Marina Boulevard, DBS Asia Central, Marina Bay Financial Centre Tower 3, Singapore 018982
Country:	Singapore
SWIFT Address/Code:	DBSSSGSG

☐ PAYNOW to:
Trade Link Media Pte Ltd

PAYNOW option is applicable for **Singapore companies only**.

Company Registration Number: 199204277K

* GST inclusive (GST Reg. No: M2-0108708-2)

ADVERTISE WITH US TODAY!

Email us at info@tradelinkmedia.com.sg.

Scan to visit our website