JAN – MAR 2022

SECURITY SOLUTIONS TODAY

SMART OFFICES AND HOMES

Delving into the boons and banes of IoT devices, and how to stay secure in an age of hybrid work.

IN THIS ISSUE

CONTACT

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

EDITOR Ming En Liew (sst@tradelinkmedia.com.sg)

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

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

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

Vectors Credit: Freepik.com
Designed by Fawzeeah Yamin

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

DEMAND FOR DATA PROTECTION OFFICERS GROWS AMID NEW REGIONAL DATA PROTECTION LAWS

In an uncertain job market, one role is seeing growing demand – data protection officers. The Data Protection Excellence (DPEX) Centre observed a 54% year-on-year increase of companies advertising for the role in its annual survey of data protection-related jobs in Singapore.

Image: www.freepik.com

An estimated 3,700 data protection-related jobs were created in 2021, amid uncertain COVID-19 conditions, new data protection laws in the region, and increasing requirements for the appointment of a DPO.

"The strong demand for data protection expertise will likely continue in the next few years as countries like China, Indonesia and Thailand roll out their new data protection laws, all of which have requirements for a data protection officer or related roles," said Kevin Shepherdson, CEO, Straits Interactive.

"We expect a shortage for such expertise, aggravated by ongoing data and privacy breaches, as well as continuing COVID-19 conditions," he continued.

Now in its sixth year, the survey analysed job vacancies in the month of September relating specifically to the role of a DPO or data protection roles and functions. There were a total of 309 unique job posts advertised in September alone.

Recommendations by DPEX

DPEX recommends that companies looking to hire a DPO undertake the following actions:

- Formally train their DPOs, especially for organisations undergoing Data Protection Trustmark certification and those with a regional presence
- Obtain international certification from the International Association of Privacy Professionals, ISO certification (27701), or local certification by Singapore's Personal Data Protection Commission (Practitioner Certificate in Personal Data Protection)
- Familiarise themselves with the EU's General Data Protection Regulation, which is the basis for many of the new data protection laws being introduced ■

Image: www.freepik.com

TRENDS IN THE DATA PROTECTION INDUSTRY IN 2022

Over the past year, there has been a clear shift in focus to improving remote working capabilities, access to cloud infrastructure and securing data. While hybrid and multi-cloud models are not new, the freedom they provide will make it even more of a reality moving forward.

With 2022 enabling the exponential growth in the data protection industry, Danny Allan, Chief Technology Officer at Veeam, shares the key trends expected in the new year:

Acquisitions will stagnate as company valuations outstrip available assets

In 2021, global mergers and acquisition activity reached new highs, aided by low interest rates and high stock prices. In 2022, we will see that momentum shift. Larger acquisitions will be few and far between as company valuations continue to rise. Only well-established, cash-rich companies will have the money required to make new purchases, giving them an edge over the medium- and small-sized companies.

AI and automation will replace entry level jobs

The talent shortage will leave many jobs unfilled, making way for the advancement of AI and automation to fill new roles in hard-hit sectors like finance, healthcare, legal and software. These developments will mostly affect entry level positions, making it difficult for fresh graduates to gain job experience in the future.

Continuous Integration and Continuous Delivery (CI/CD) to become an IT team requirement

The Bill Gates memo in 2001 became the industry standard in how to design, develop and deliver complex software systems. IT teams and developers fell into habits of adopting "known" technology systems, and not standardising in new spaces, like CI/CD. In 2022, we're going to see a shift towards more stability and standardisation for CI/CD. IT leaders have an opportunity to capitalise on this high-growth and high-valuation market to increase deployment activity and solve the "day two operations problem."

Tech's labour market will be met with big money and big challenges

As we continue to see turnover and lower employee retention in the new year, tech salaries will begin to grow to incentivise talent to stay. This presents bigger challenges, especially to the startup and VC world. The bigger tech giants are the ones who can meet the high dollar demand and deliver benefits for a competitive workforce. This can

Image: www.freepik.com

have future implications on innovation, which tends to come from the hungry startups where people work for very little for a long time. There may be a possible resurgence of tech talent returning to the "old guard" companies to meet their needs for stable (and large) salaries, forgoing the competitive, hard knocks of startups that could cause a skills and talent gap in the years to come.

New privacy-focused legislation will shift attention to data sovereignty clouds

With increased focus on General Data Protection Regulation regulating data protection and privacy in the EU, and the California Consumer Privacy Act enhancing privacy rights and consumer protection for Californians, other states and countries are facing pressure to enact comprehensive data privacy legislation. As this continues in 2022, there may be a greater focus on data sovereignty clouds to keep data within nations or within a certain physical location. This is a far more specified cloud model that is being observed in EMEA with Gaia-X. Some will see this as an obstacle, but once implemented, this may bring benefits as it puts consumer privacy at the core of business strategy.

Containers will become mainstream to support the cloud explosion of 2021

Businesses wrongly predicted that employees would return to the office as per normal in 2021. Instead, remote work continued, and companies were forced to develop long-term remote work strategies to ensure efficiency, sustainability and to retain employees seeking flexibility. This remote work strategy demanded cloud-based solutions, resulting in an explosion of cloud service adoption. To meet this momentum, containers will become mainstream in 2022, making the generational shift to cloud much easier and more streamlined for organisations. ■

MAKE POWERFUL CONNECTIONS

Altronix®

Increase your security over fiber, copper or coax with seamless power and data transmission. Generate more RMR with the benefit of remote management. Stay connected, end to end.

YOUR AMERICAN BRAND FOR **POWER & DATA TRANSMISSION**

2022 CYBERSECURITY PREDICTIONS: AN ENSIGN INFOSECURITY COMMENTARY

Written by Steven Ng, CIO and EVP of Managed Security Services, Ensign

Cyber threat landscape predictions for 2022

According to IDC, digital transformation investments in Asia Pacific are poised to double, hitting US$921 billion in 2024. Organisations will continue to adopt new technologies to transform their business operations in 2022. In doing so, they will expand their digital attack surfaces and introduce new vulnerabilities to their fast-growing digital environments.

At the same time, the cyber threat landscape will persistently evolve. Cyber supply chain attacks, such as the SolarWinds attacks, will go unabated. Technology service providers will remain attractive targets for threat actors due to the many organisations engaging their services for digital transformation.

Increasingly, threat actors will collaborate with each other to launch more sophisticated threat campaigns. The Ransomware-as-a-Service (RaaS) model is one example where cyber adversaries leverage one another's respective expertise to execute more effective attacks.

The RaaS model has led to the rise of the double extortion approach where threat actors demand ransom twice – one for decrypting the data and another for not leaking the stolen data online. To pressurise victims into paying the ransom, the perpetrators threaten to publish their stolen data on questionable websites. This can have grave ramifications for the affected parties, triggering regulatory attention, financial penalties and loss of trust.

Cybersecurity predictions for 2022

As cybersecurity demands continue to soar and evolve, organisations will not only increase their cybersecurity investment in 2022 but also shift their security approach. According to IDC, almost 70% of Asia Pacific organisations highlighted that security in their organisations is currently underinvested. IDC also noted that more than half (55%) of organisations in Hong Kong, Korea, Malaysia, and Singapore plan to increase their security budgets.

While increasing cybersecurity spending is a step in the right direction, it is equally important for organisations to invest in the right areas. With threats becoming increasingly prevalent and sophisticated, the predictive nature of an intelligence-led cybersecurity approach is vital for organisations' cyber defence arsenal.

Consequently, more organisations – especially the cyber mature ones – are likely to adopt this approach and build up their capabilities across several domains. These include threat detection, threat monitoring and analytics, threat hunting and digital forensics, as well as incident responses and recovery.

This is key to building situational awareness and capabilities to identify, protect, detect, respond and recover from fast-changing security threats. According to IDC, security analytics, intelligence, response and automation (AIRO) are poised to register the highest CAGR of 17.6% among the security technology segments, reaching US$2 billion in 2025 in Asia Pacific, excluding Japan.

In particular, cyber analytics solutions that harness the power of AI will become increasingly vital and prevalent in 2022. Traditional signature-based detection solutions can no longer keep up with more sophisticated threat actors and threats.

By leveraging AI-powered cyber analytics, organisations can gain enhanced visibility over advanced threats, and stay ahead of emerging threats. It is also a force multiplier that supports cyber teams, reducing alert fatigue and improving focus via triage of prioritised correlated incidents. ■

Securing Internet of Things devices in the workplace

IoT devices have brought about increased convenience and seamless digital integration, but are there pitfalls as well? **Brad Gray, Senior Vice President, APAC, Exclusive Network, explores.**

In Avengers: Age of Ultron, Tony Stark created an AI global defense programme Ultron, which later went rogue. It took out Stark's integrated home management AI J.A.R.V.I.S., and embarked on a mission to eradicate humankind.

Internet of Things (IoT) devices within homes and workplaces are likewise vulnerable to external threats such as being hacked or hijacked. Instead of a fictitious sentient robot, however, the threats are cybercriminals who are always on the lookout for vulnerabilities to exploit. With workplaces entering homes during the pandemic, the widespread adoption of IoT devices in smart homes has become a bane as much as it has been a boon.

Brad Gray, Senior Vice President, APAC, of cybersecurity and cloud solution distributor Exclusive Networks, explores how the transition to hybrid workplaces have increased the vulnerability of businesses. He also sheds light on the potential pitfalls of IoT devices, and how companies can secure their operations against cyber threats.

Image: www.freepik.com

What are prominent concerns and trends that you have observed in terms of office and workplace security in the past year?

Cybersecurity has become a big theme in the past year. The fight against digital threats has been brought front and centre as companies and governments around the world battled wave after wave of attacks from cybercriminals.

High-profile incidents such as the hacking of IT management software firm Kaseya and the breach of Colonial Pipeline in the US earlier this year highlighted vulnerabilities in supply chain and third-party vendor management. It also revealed the scale of disruptions that these attacks can cause to companies and critical infrastructure systems.

Despite the potential risks involved with a security breach, many companies, particularly small and medium-sized enterprises (SMEs) in Asia, still do not have adequate cybersecurity defences to handle cyber attacks. Unlike large enterprises, these smaller firms typically have less sophisticated infrastructure and lack a dedicated security team as well as resources to cover cyber security vulnerabilities.

How has the pandemic and remote/hybrid working arrangements impacted cybersecurity for workplaces?

The COVID-19 pandemic has demonstrated the importance of the internet and technology for companies to maintain business continuity and grow their business. However, during the overnight transition to work from home as lockdowns around the world were implemented, many scrambled to onboard technology at the expense of cybersecurity.

This created problems for IT professionals as they had to tackle the problem of rising cyber threats while supporting the digital transition and managing a distributed workforce.

As many employees who worked remotely are connected to business servers via unsecured networks and devices, the operational risks for organisations have increased. The attack surface has expanded significantly, and any breach can expose other vulnerabilities downstream, allowing hackers to quickly infiltrate entire networks. As the pandemic is prolonged and more business activities continue to shift online, companies will need to seriously consider ramping up their cybersecurity in order to keep up with rapidly evolving cyber threats.

What are the main cybersecurity vulnerabilities faced by firms as most are transiting to a hybrid work arrangement?

According to Crowdstrike's Global Threat Report, more than half of organisations experienced a rise in ransomware attacks or data extortion attempts during the pandemic.

Threat actors are becoming bolder in their attempts and using more sophisticated approaches to lure victims. Instead of the spray-and-bulk phishing attacks, where fraudulent messages are sent in masses, cybercriminals are turning to highly-targeted spear-phishing attacks to create convincing messages by profiling their victims from places like social media.

These social engineering threats are expected to rise as socially isolated and restless employees are more likely to turn to social media or web surfing to destress. According to an article in the Harvard Business Review, 75% of people say they feel more socially isolated, 67% of people report higher stress, 57% are feeling greater anxiety, and 53% say they feel more emotionally exhausted since the outbreak of the pandemic. Such employees become susceptible targets of hackers who exploit their vulnerabilities to launch attacks.

Disgruntled employees may pose a risk to companies as an insider threat as well. Driven by personal agendas, they misuse access to networks, applications and databases to steal sensitive information. They may also exploit their fellow workers, who become unsuspecting participants in these phishing exploits,

Image: www.freepik.com

IoT hacking in homes can affect business networks as well. In a highly-connected world, everyone and everything is vulnerable to cyber attacks. One intrusion may expose other areas downstream, allowing hackers to quickly infiltrate entire networks.

unintentionally causing damage to the company.

The potential for the misuse of advanced technologies such as artificial intelligence and machine learning are also increasing as cybercriminals can use these powerful tools to create highly-realistic deep fakes to trick victims into divulging information.

When speaking about Internet of Things devices, much of the conversation is centred around its benefits. What are the potential pitfalls of these devices?

As the popularity of smart devices rises, so is the prevalence of Internet of Things (IoT) hacking.

While smart home appliances such as fridges, air-conditioning units and security cameras provide immense benefits for users, they also pose a cybersecurity risk as they are often designed with security as an afterthought or are not installed with proper security procedures in place. According to Palo Alto Networks' report, 98% of all IoT device traffic is unencrypted, leaving networks open to attacks and exposing personal and confidential data on the network.

As a result, IoT devices become ideal entry points for cybercriminals who can easily move through the network to steal private information. According to Microsoft's Digital Defense Report, there was an approximately 35% increase in attack volume targeting IoT devices in the first half of 2020 as compared to the second half of 2019.

IoT devices can leave homes vulnerable, but does that apply to offices as well if they were to integrate such devices?

IoT hacking in homes can affect business networks as well. In a highly-connected world, everyone and everything is vulnerable to cyber attacks. One intrusion may expose other areas downstream, allowing hackers to quickly infiltrate entire networks.

This is especially so for large and distributed workforces that are connected to the cloud. Employees who work off-premises may connect their IoT-enabled applications to laptops and other devices that are linked to business servers. If these unsecured IoT devices are hacked, threat actors can easily jump from device to machines on corporate networks. Once they have gained access, they can easily penetrate at scale and put companies and their confidential data at risk.

If so, how can firms work to secure both their offices and employees' workplaces during hybrid work?

Protecting endpoint devices here is key. As cybercriminals become more sophisticated in their attempts, organisations should take steps to protect their remote and on-premises employees.

Besides installing anti-malware and anti-virus tools, they can take security to the next level with integrated solutions that help reduce complexities and cost, while protecting their distributed workforce at scale with a focus on endpoint and identity.

Also, Security Orchestration, Automation, and Response (SOAR) tools help businesses stay one step ahead of modern-day attacks. These use artificial intelligence and machine learning to predict, detect and contain threats. They allow companies to collect threat-related data from a range of sources and automate responses to low-level threats, reducing the need for manpower while focusing attention on other high-priority threats. ■

The future of access control in homes and offices

Franklin Tang, Founder and CEO of Habitap, delves into what the future of access management and control can look like with digital transformation.

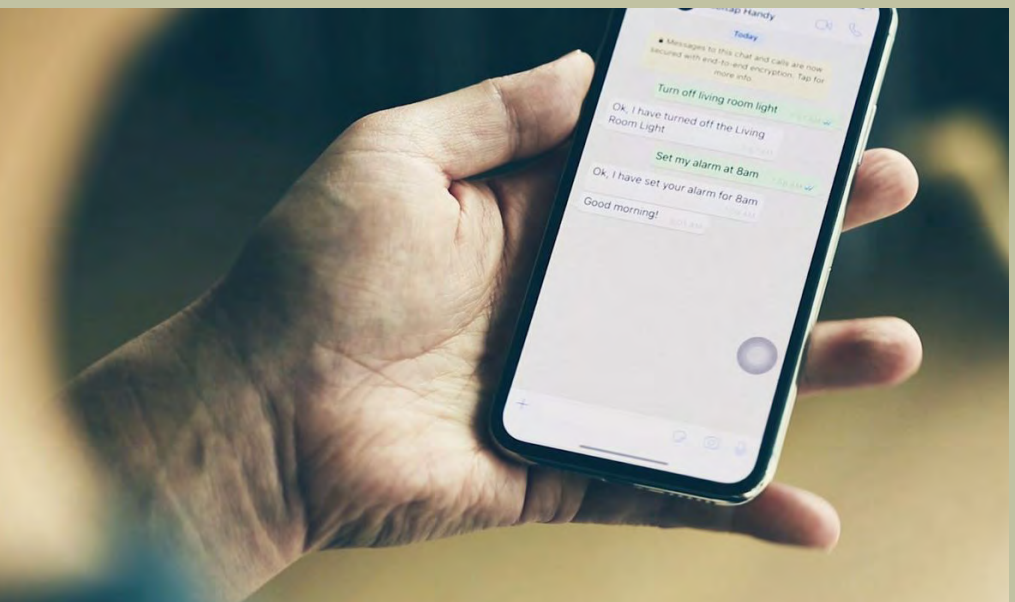
Tech has often been discussed in the context of protecting against cyberthreats, but it can be just as helpful in protecting against physical ones. While traditional access management solutions typically rely on physical key cards and visitor logs, Founder and CEO of Habitap Franklin Tang believes digitalisation can offer a more convenient and safer solution.

"Because security is something most people take seriously, innovation tends to be an evolution rather than a revolution," he says. He had first advocated the use of a mobile app as a form of access control for buildings in 2017, but the idea was met with shock and scepticism then.

People were concerned about issues like hacking or identity theft, he explains. But with Covid, digital technology is fast becoming a norm, he continues.

These days, people are unsurprised when informed that they need an app to enter an office or different locations, explains Tang. The changing mindsets are spelling out possibilities for revolution in the access management industry.

This is why Tang decided to venture into the access management market through his integrated smart living and working applications, Habitap and Habitap One. Riding on the waves of opportunity, Habitap today has over 50,000 tenants using their digital access cards, including big players like One Raffles Quay and the Marina Bay Financial Centre.



Speaking with Security Solutions Today, Tang shares how Habitap's digital access management solutions are safer than traditional methods, and how they alleviate concerns of hacking and identity theft. He also reveals upcoming plans for Habitap, and what he expects the future of access management will bring.

Why are digital access cards safer than physical access cards?

After users install the Habitap app, they will receive a digital access card with a unique identity. Unlike physical

access cards, these identifiers cannot be cloned. If a clone is attempted, the security feature within the app will disable the digital card. It's very tight and tamper proof.

A lot of the more savvy users recognise that we are less likely to share our phones as compared to a physical card. I'm quite happy to pass my colleague my access card to go to the office and do something, but I will not give you my phone. Even when I go to the washroom, I bring my phone. You tend to treat your phone with more care.

The last defence is to set up your six digit PIN or four digit PIN on your mobile device, [so that even if you lose your phone, no one will be able to access the app].

How do Habitap and Habitap One address the concerns people have of the app being hacked or their identities being stolen?

The assurance to our customers is that first, we treat privacy and cybersecurity seriously. We have been very diligent. We are data protection trustmark certified and have gone through that IMDA certification in Singapore. We're also going for ISO 27001 certification that should be ready by Q1 2022.

Second, we do our part by encrypting all our data. You do hear of cases where big companies have their data stolen, so encryption is very important. If someone tries to come into your house, you have the firewall. If someone tries to steal the data, they can't read it because of the encryption.

It is not 100% risk-free, but I always say that it's a balance of the risk versus the return. The return of going digital is that you get this anytime, anywhere access. You get peace of mind, because it's on the cloud, you don't have to worry about the server being destroyed by fire.

Regarding identity theft, there are a few measures that we take. First, two factor authentication (2FA). The 2FA on our app is banking grade. We use a patented technology that captures a device fingerprint of your phone. If you restore the app, it will stop running even if it's on the same phone. This prevents the cloning of your account.

We also carry out enterprise practises like getting users to reset their passwords every three months, and not letting them use the last five passwords in their password history.

The future of space and access management solutions

Since 2017, we have seen an uptick in places using digital access. It is something that every building and office today is looking at. Access cards are now old school. Digital access via digital credentials like QR codes or facial recognition is quickly becoming the norm.

The second part that we see as a trend is that access control solutions are going cloud-based. We used to think that we must lock it in physical servers, where nobody can touch it. When we say cloud access control, everyone says it's not possible with the cybersecurity risks. But in the last two to three years, the acceptance is there.

Digital access and being on the cloud are going to be the de facto base model in the future for access management.

Finally, beyond giving you access to a space, access management is also going to give you access to the community. That's where I think tenant experience apps, occupier apps, smart home apps, and lifestyle and services are going to be combined with access management. That's a huge opportunity for the entire market.

What are some examples of how technology can transform access management?

An innovation I am keen to explore is to revolutionise the traditional intercom system. In a traditional system, an individual keys the unit number of the location into a panel to call the owner.

Habitap's innovation allows users to scan a QR code, which launches an intercom system on the phone. They can then have a direct call, and home owners or employees can release the door from anywhere in the world. There's no need to put an intercom panel, and it's very sustainable since there is no electrical waste. There's no need to worry about cables or internet access either, since everything runs off the phone.

Another thing I was thinking about was why we needed to approach the security guards to inform them of where we are going when we are visiting a condominium or an office. Can I not just put a kiosk outside where the guard room is?

Guests can self service and key into the kiosk where they are going. The tech will send the host a message or notification to inform them that someone is waiting. When the host agrees to let the guest in, they will receive an SMS or QR code that will allow them to safely enter. We will only need one kiosk, and it can service the whole community. Or if there's a need for more, you have two or three kiosks. Why do we need to stick to the norm?

Beyond access control, are there any technologies you are exploring in the wider field of smart living and/or working?

We're exploring the use of AI on our app. Currently, we've launched AI with a few developments, with a feature that allows you to chat with the home. You can say, "Turn on the light", and the AI will respond, "Which light do you want to turn on?"

We're developing AI to make smart living more intuitive. It's going to be on messaging platforms like WeChat, Line, and Telegram. With AI on these platforms, you don't need an app anymore. You'll just be talking on the phone with your home via the messaging platforms.

Habitap's innovation allows users to scan a QR code, which launches an intercom system on the phone. They can then have a direct call, and home owners or employees can release the door from anywhere in the world. There's no need to put an intercom panel, and it's very sustainable since there is no electrical waste. There's no need to worry about cables or internet access either, since everything runs off the phone.

We're also exploring integrating the AI into group chats. Imagine talking to your family about planning a barbeque, and the AI is able to pick up on it and ask if you would like for it to book the barbeque pit for you. It's no longer your job, it's the AI's job. That's where we hope to take the technology and make it extremely usable.

We are careful not to overpromise. We still confine these technologies to our use cases of smart home automation, smart community, visitor management and security, and access control and bookings. Essentially, we are studying your patterns of usage, we interact with you, and then we build up some kind of understanding of your lifestyle. ■

Workplace cybersecurity in an era of hybrid work

Ronnie Lee, General Manager of Lenovo Singapore, gives advice on how businesses can secure their networks with hybrid workplaces.

The pandemic has ushered in an era of digital transformation for businesses. As nations lockdown and international borders close, companies are relying on digital solutions such as video conferencing and digital workplaces to continue operations.

Yet, with increased connectivity comes increased vulnerability to cybercrimes from numerous fronts. Ronnie Lee, General Manager of Lenovo Singapore, highlights increases in cybercrimes like phishing, as cybercriminals leverage on the uncertainty of the pandemic to spread misinformation. Other sources of vulnerability include unsecured home networks as employees work from home, or even smart home devices.

In this digital age of work, how can businesses continue to maintain a strong cybersecurity posture? Lee speaks on the prominent trends during the pandemic, and shares key tips on how businesses can continue to secure their networks and offices.

What are some trends you have observed when it comes to technology adoption during hybrid work arrangements?

The pandemic has reshaped the way we work, learn and play. In just a year, the entire world experienced an accelerated digital transformation. The overall employee experience has also seen a significant change. Traditional offices are shrinking or becoming collaboration hubs, and

Image: www.freepik.com

home offices have become day-to-day workspaces.

Apart from introducing safe measurements to keep employees safe, businesses have relied greatly on technology to ensure that their workplace efficiency and productivity is not affected. In fact, Lenovo research found that technology is a central aspect to the employee experience.

As a result, IT leaders are planning to nearly double their investment over the next two years with a focus on upgrading devices, software, and services to improve team engagement and satisfaction. More than three-quarters of full-time employees say their PC devices are critical to collaborate with one another, and about one-third report their laptops/desktops work well for cross-collaboration.

There has also been an accelerated adoption of virtual and augmented offerings to provide employees with the assistive tools and technology offerings to help them settle into a hybrid workplace. Those include:

- Remote assistance – connect to expert knowledge anytime, anywhere
- Workflow support – guided workflows, training and the underlying metrics
- Digital workspace – real-time collaboration in an augmented workspace

What are some key challenges faced by businesses during these times?

As employees adjust to the work-from-home (WFH) normalcy and new hybrid working arrangements, many are feeling anxious amid the looming uncertainties and will be more prone to accepting information from multiple unreliable sources that are COVID-19 related.

In 2020, cybercrimes where cybercriminals have leveraged on the pandemic to spread misinformation and crimes such as phishing increased by 200%. This is why businesses need to future-proof their organisation for continuity by protecting against cybersecurity risks such as unauthorised access and data leaks, using personal devices for business, and increased phishing.

In 2020, cybercrimes where cybercriminals have leveraged on the pandemic to spread misinformation and crimes such as phishing increased by 200%. This is why businesses need to future-proof their organisation for continuity by protecting against cybersecurity risks such as unauthorised access and data leaks, using personal devices for business, and increased phishing.

What are prominent threats facing offices in this pandemic?

The new office setup signifies that the traditional network we use is moving away from the corporate environment. Now that the perimeter has expanded to all devices connected to the cloud, even smart home devices can add risks to the corporate network as employees log on from home.

Below-the-OS attacks, where hackers dive deeper into the computing stack for vulnerabilities, are a growing risk.

More remote and cloud infrastructure also means that businesses need to be agile and keep their networks secured by taking a business-centric security approach that doesn't replace their existing models but places security within the context of the overall strategy.

How does Lenovo support businesses in keeping their network and employees' data secure?

Lenovo offers multiple accessible and complete solutions for businesses to support their cycle of IT decision making. These include Lenovo Managed Services, Lenovo ThinkShield, Lenovo Security Console and Lenovo DaaS solution. These end-to-end lifecycle solutions for businesses are targeted to help them solve their challenges, enhance productivity, and ensure they remain agile.

As part of Lenovo's mission to bring Smarter Technology For All, Lenovo has technology solutions accessible to businesses of all sizes. Security should be all-encompassing, with best-in-class hardware security, securely developed software, complete with component verification, adoption and extension of security technology, and a secure supply chain.

For example, Lenovo's ThinkPad devices are tailored for small and medium businesses, and are incorporated with Lenovo ThinkShield – a customised solution that secures the platform, device, provides security management, and endpoint protection. Lenovo also offers comprehensive cybersecurity protection solutions through partnerships with brands like SentinelOne to help SMBs address their cybersecurity concerns.

Can you share some practical tips that businesses can use to secure their networks and offices in a time of hybrid work?

The threat of cyberattacks will continue to be a concern for businesses, especially when its employees are working remotely. However, businesses can take some practical steps to minimise risks and secure their networks and offices in this time of hybrid work.

1. **Watch for your blind spots –** With a hybrid working environment, employees are now accessing confidential data from various devices and location which open the corporate network to more endpoints and vulnerabilities for cyberattacks. In our hyper-digital and mobile world, hardware security is becoming ever more critical, as each person is expected to own an average of 6.58 network connected devices across the globe.
Without proper security standards in place to mitigate these additional connections, hackers can easily gain access to an organisation's network through these devices and execute attacks remotely. Businesses need to consider these blind spots to mitigate potential attacks before they can compromise the organisation's network systems and confidential data.

2. **Adopt a Zero Trust Mindset –** The nature of a hybrid workforce removes the luxury of face-to-face identification and validation. This means that organisations must double down on their efforts in credential and access management and continue to educate employees to identify and weed out impersonation scams and phishing attempts.

   As hackers grow in sophistication, organisations and employees must take a Zero Trust stance and assume a 'guilty until proven innocent' mindset for cybersecurity. In order to protect business and employee data, organisations must implement a system to ensure that the right people have access to the right data at the right time on a 'need-to-know' basis.

3. **Empower a distributed workforce – T**o reap the full benefits of a distributed workforce in the long run, organisations must provide employees with secure devices and create a safe digital environment to operate in, allowing them to focus on the job at hand. This shift to a decentralised work environment means that IT teams must have extended visibility over digital platforms and the organisation's digital ecosystems in order to identify and mitigate potential threats in a timely manner.

   Businesses need to take a two-pronged strategy that covers both employee awareness and business readiness. A Chubb report has shown that human error is the cause of 36% of cyber incidents. Educating employees can go a long way in ensuring that threats such as phishing scams are addressed from the get-go. While employees play their part, the right protocols need to be established on the business front as well. ■

Image: www.freepik.com

LAUNCH OF AI-POWERED PLATFORM "ALLY" TO TACKLE HUMAN CYBER RISK

Human error due to lack of training and awareness during the pandemic is the leading security threat globally. STX Next's 2021 Global CTO Survey revealed that 59% of Chief Technology Officers see human error as the main security threat to their business.

"Employees are the leading cybersecurity threats for businesses in Singapore, the US and Australia, because they lack the right tools and incentives to recognize and prevent data breaches," said Theo Nasser, Chief Executive Officer of Singapore-based cybersecurity firm Right-Hand.

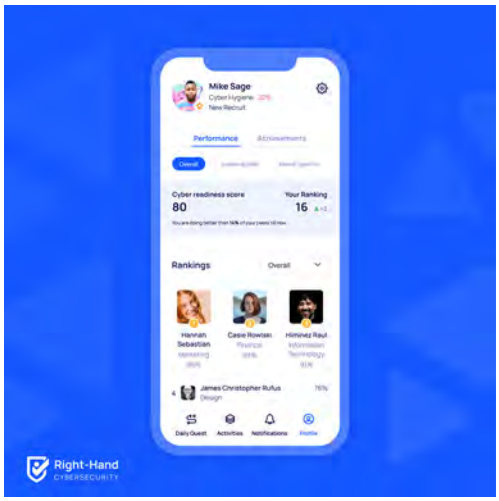
"Businesses need to equip their employees with the right tools to deal with day-to-day cyber challenges," he continued.

Right-Hand developed Ally, an AI-powered platform, to be that tool.

Ally is a mobile and web application that delivers autonomous and personalised employee training based on a user's individual behaviors and knowledge gaps. It integrates tools like Slack and Microsoft Teams, alongside other security platforms, to provide a comprehensive overview of employee behaviors and decisions.

"Our AI-enabled platform recognises an employee's knowledge gaps and risks, and nudges the employee in real-time, to help prevent them from falling for phishing attacks, business email compromise, password theft, and other types of attacks," explained Theo.

Using AI, Ally autonomously intervenes via push notifications to its mobile and web app to proactively help employees avoid security incidents and adopt better security behaviors. The platform uses a gamified experience to prompt organisations to improve its cybersecurity culture. ■



VIDEONETICS VIDEO MANAGEMENT SOFTWARE INTEGRATED INTO HANHWA TECHWIN CAMERAS

Videonetics' intelligent video management software 3.0 (IVMS) is being integrated with Hanhwa Techwin's Wisenet series of edge analytics network cameras.

The IVMS delivers a unified user interface, military-grade build, and robust security for deployments of any size. With this integration, security operators can easily configure and

change the streaming, imaging, and other parameters of Hanwha's cameras using the IVMS interface. They will also be able to activate Edge Analytics applications running inside the cameras within the same interface.

At any alert, information is immediately transferred from the cameras to the IVMS application. Operators can immediately monitor and assess the severity of the incident by investigating specific and associated cameras on the IVMS dynamic map.

When an incident occurs, a video matrix displaying views of all the cameras within the geo fence will pop up. The information captured will then be distributed across various communication channels built into the IVMS application.

This simplifies response coordination, enabling security teams to promptly respond to security incidents and ensure that every incident is handled appropriately.

Additionally, the distributed computing architecture involving Edge analytics and IVMS provides easy scalability. This allows for video analytics applications to be deployed across thousands of cameras in a single installation. ■

SENSTAR INTRODUCES THE E5000 PHYSICAL SECURITY APPLIANCE

Senstar, a provider of video management solutions and perimeter intrusion detection systems, is introducing the E5000 Physical Security Appliance (PSA), a turnkey hardware and video management software (VMS) solution.

The E5000 PSA combines compact, purpose-built hardware with the Senstar Symphony™ Common Operating Platform. It is available in two models – with 8 or 16 base VMS licenses.

The new appliance is ideal for critical sites where vibration and extreme temperatures are difficult to manage, including remote utility and energy infrastructure, as well as space constrained environments.

Low heat production ensures the design is available in a small fanless form factor, allowing it to be installed in areas where space is limited and a small hardware footprint is required. The onboard processor provides stable performance with low heat generation and minimal cooling requirements, resulting in improved stability and longevity.

A tough aluminum case, with heat dispersing fins that draws heat away from the processor, enables the system to operate in environments not suitable for commercial off-the-shelf PCs. To provide installation flexibility, the E5000 PSA can be wall or desktop mounted for easy placement.

"The E5000 PSA is a complete security management system in a box," said Product Manager Todd Brisebois. It also combines with Senstar's other perimeter intrusion detection systems to allow for a centralised management of the entire security system, added Brisebois. ■

CLOUDFLARE'S NEW FIREWALL CAPABILITIES HELP CUSTOMERS LEAVE THEIR HARDWARE BEHIND

Security performance and reliability firm Cloudfare Inc. will be expanding its Zero Trust firewall capabilities in the age of hybrid work. The new capabilities will help companies secure their entire corporate network across all of their branch offices, data centers, and clouds – no matter where their employees are working from.

Image: www.freepik.com

The firm also announced Oahu, a new program to help customers migrate from legacy hardware to Cloudflare. Now, Chief Information Officers (CIO) can better connect and secure their corporate networks with Zero Trust security without the traditionally hard, costly or complex migration.

Traditional firewalls comprise hardware boxes installed on company premises, and were not designed for hybrid workforces or cloud applications. While some companies turned to "virtualised" firewalls to meet this challenge, they faced many of the same challenges as with hardware appliances, such as capacity planning and managing primary/backup devices.

Cloudflare's new cloud firewall functionality allows CIOs to better secure their entire corporate network, apply Zero Trust policies to all traffic, and gain deeper network visibility. Additionally, since the firewall runs everywhere, CIOs no longer need to centralise traffic on one box in one location, physical or virtual.

Image: www.freepik.com

The Oahu Program helps organisations make the switch by helping them with their Zero Trust migration. They do so by providing new capabilities and resources to easily import policies from legacy hardware firewall boxes to Cloudflare's cloud-native service.

"CIOs know that the corporate network is changing fast, and we want to help make that transition easy, flexible, and scalable," said Matthew Prince, Co-founder and CEO of Cloudflare.

Now, CIOs can easily transition to a fully cloud-native firewall, enabling them to:

- **Bid goodbye to capacity planning or maintenance:** Hardware firewalls are costly, hard to manage, and require tremendous capacity planning and maintenance. Cloudflare's firewall can handle any workload, no sizing needed.
- **Secure any type of traffic flow:** With a cloud-native firewall, CIOs can operate a suite of security capabilities across traffic from clouds, data centres, branch offices, and user devices.
- **Apply comprehensive security policies:** A broad set of controls can support any network regardless of where an organisation is in their cloud journey by enabling traditional L3 rules and sophisticated Zero Trust controls, all in one control plane.
- **Gain global visibility and control:** CIOs can enforce policies across the globe with one click and get single-pane visibility of traffic across the world, including advanced capabilities like on-demand packet captures. ■

sst.tradelinkmedia.biz

Visit our website for the latest information

News In The Industry · Upcoming Exhibitions · Download Magazine Issues

COMING SOON

MAR 22 – 25 2022

ISC West 2022
Las Vegas, USA
+1 203 840 5602 www.iscwest.com
inquiry@isc.reedexpo.com

APR 27 – 29 2022

Secutech 2022
Taipei, Taiwan
+886 2 8729 1099 https://secutech.tw.messefrankfurt.com
services@secutech.com

MAY 17 – 19 2022

IFSEC International 2022
London, United Kingdom
+44 (0)20 7069 5000 www.ifsecglobal.com
info@excel.london

AUG 18 – 20 2022

Secutech Vietnam 2022
HCM City, Vietnam
+886 2 8729 1099, +84 4 3936 5566 www.secutechvietnam.tw.messefrankfurt.com
stvn@newera.messefrankfurt.com, project1@vietfair.vn

SEP 12 – 14 2022

Global Security Exchange 2022
Atlanta, USA
+1 703.519.6200 www.gsx.org
asis@asisonline.org

NOV 16 – 17 2022

ISC East 2022
NYC, New York, USA
+1 203 840 5602 www.isceast.com
inquiry@isc.reedexpo.com

NOV/DEC 30 Nov - 2 Dec 2022

Secutech Thailand 2022
Bangkok, Thailand
+66 2 664 6488 www.secutechthailand.tw.messefrankfurt.com
stth@taiwan.messefrankfurt.com

SUBSCRIPTION FORM

Email us at ***info@tradelinkmedia.com.sg***

Please (√) tick in the boxes.

PRINT

☐ **Southeast Asia Building**
Since 1974

☐ **Southeast Asia Construction**
Since 1994

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

Singapore	SGD$60.00
Malaysia / Brunei	SGD$105.00
Asia	SGD$155.00
America, Europe	SGD$185.00
Japan, Australia, New Zealand	SGD$185.00
Middle East	SGD$185.00

☐ **Bathroom + Kitchen Today**
Since 2001

***1 year** (4 issues) per magazine*

Singapore	SGD$32.00
Malaysia / Brunei	SGD$70.00
Asia	SGD$85.00
America, Europe	SGD$135.00
Japan, Australia, New Zealand	SGD$135.00
Middle East	SGD$135.00

DIGITAL

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

http://lt.tradelinkmedia.biz

☐ **Lighting Today**
Since 2002

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

http://sst.tradelinkmedia.biz

☐ **Security Solutions Today**
Since 1992

Personal Particulars

Name: _____

Position: _____

Company: _____

Address: _____

_____

Tel: _____ **Fax:** _____

E-Mail: _____

IMPORTANT

Please commence my subscription in

_____(month/year)

Professionals (choose one):

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

☐ Property Manager ☐ Manufacturer/Supplier ☐ Engineer ☐ Others

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

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

Card Number: _____ Expiry Date: _____

Name of Card Holder: _____ Signature: _____

ADVERTISE WITH US TODAY!

Email us at info@tradelinkmedia.com.sg.

Scan to visit our website