A Canalys Special Report

ASEAN MSPs are key to customers' data protection

How can ASEAN MSPs protect themselves and their customers?

Commissioned by Datto

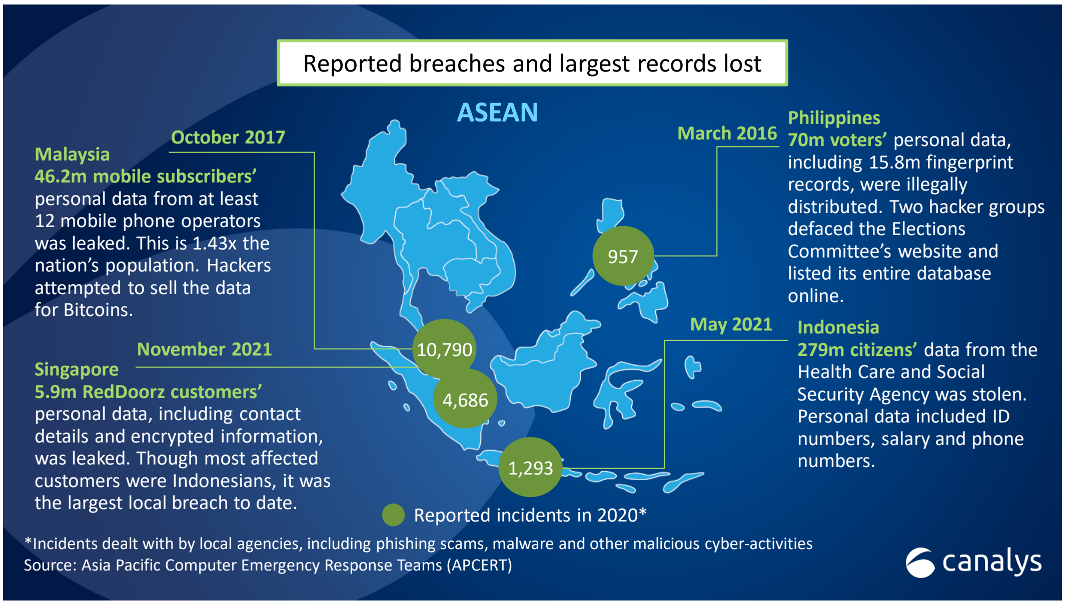
February 2022

The Association of Southeast Asian Nations (ASEAN), like other regions, has seen a large increase in threat activity aimed at Managed Service Providers (MSPs) as cyber-criminals exploit vulnerabilities in infrastructure, software and processes to access and compromise sensitive customer data. Public regulations and private cyber-insurance requirements will be among the key drivers for raising IT service and security standards worldwide. Cyber-resilience, which refers to the ability to devise policies, detect abnormal activities, respond to incidents and implement recovery plans, is an important differentiator for the growing number of MSPs in the region. MSPs must develop their own cyber-resilience as customer complexity increases. Demand for secure services across a broader range of technologies will push IT service providers to seek efficiencies and boost margins.

Safeguarding an increasingly digital ASEAN

The ASEAN region is socially and economically diverse, with a population of over 660 million people and a combined GDP of more than US$3 trillion. Countries in the region are among the fastest growing in the world and are forecast to collectively add US$1 trillion to GDP over the next 10 years. Not only is the region economically important for financial services, oil and gas, shipping, healthcare, and business process outsourcing industries, among others, but it also has some of the world's highest digital use in terms of Internet user numbers and total time spent online. Organizations in the ASEAN region are increasingly targeted by threat actors and cyber-criminals, especially as digital transformation and cloud services adoption accelerates, expanding the potential attack surface, as new vulnerabilities and zero-day exploits emerge. Governments and organizations are realizing the scale of the issue and the urgent need to enhance cybersecurity resilience.

Between 2018 and 2020, nearly 400 million personal data records were compromised in just 63 publicly known breaches in the ASEAN region. Public government organizations, with their access to highly sensitive demographic data, including personal identification numbers, and electoral and medical records, were the most targeted in terms of attack size and sophistication. But private organizations


Reported breaches and largest records lost

October 2017
Malaysia
46.2m mobile subscribers' personal data from at least 12 mobile phone operators was leaked. This is 1.43x the nation's population. Hackers attempted to sell the data for Bitcoins.

November 2021
Singapore
5.9m RedDoorz customers' personal data, including contact details and encrypted information, was leaked. Though most affected customers were Indonesians, it was the largest local breach to date.

March 2016
Philippines
70m voters' personal data, including 15.8m fingerprint records, were illegally distributed. Two hacker groups defaced the Elections Committee's website and listed its entire database online.

May 2021
Indonesia
279m citizens' data from the Health Care and Social Security Agency was stolen. Personal data included ID numbers, salary and phone numbers.

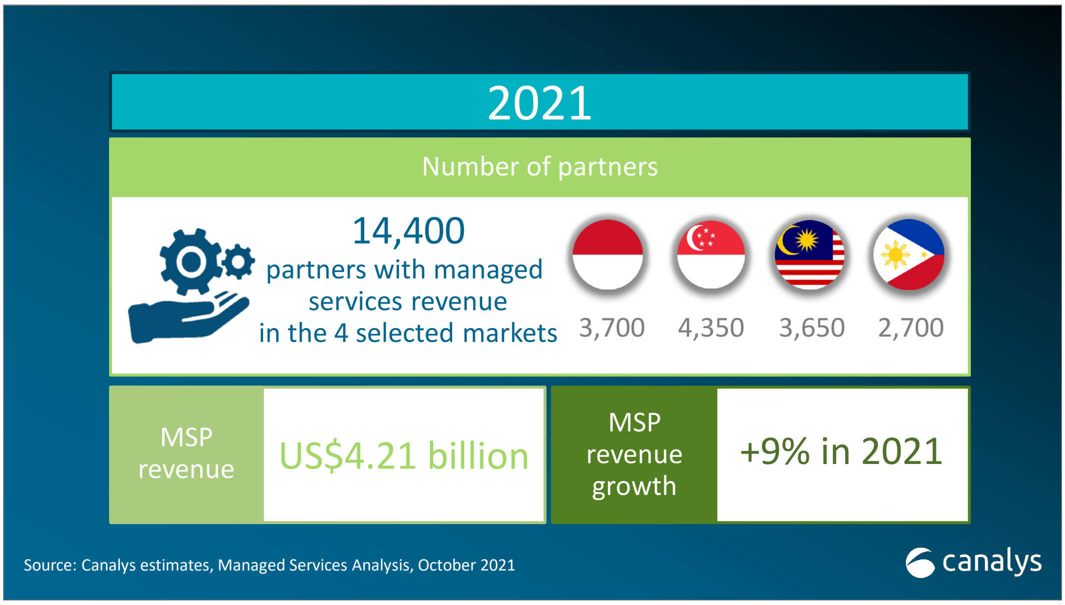
● Reported incidents in 2020*

*Incidents dealt with by local agencies, including phishing scams, malware and other malicious cyber-activities
Source: Asia Pacific Computer Emergency Response Teams (APCERT)

are not immune, as the recent surge in ransomware attacks has demonstrated vulnerabilities. In the first three quarters of 2021, Indonesia and Singapore experienced their largest data breaches in terms of records leaked, while Malaysia saw a 300-fold increase in compromised records compared to the whole of 2020. The most concerning aspect, however, is these breaches are a limited view of the overall crisis. Like the rest of the world, there is no sign of this slowing in the ASEAN region, especially with the rapid shift to perimeterless IT and acceleration of digital transformation projects.

Five reasons why cyber-resilience is important for MSPs

MSPs play a pivotal role in reducing the complexity of IT operations for customers, which has increased due to digital transformation. They have been central in helping organizations, including managing the transition to cloud infrastructure and software services, enabling distributed workforces, and implementing data protection policies. MSPs are also playing a more influential role in planning, deploying and managing cybersecurity solutions for customers. All partners, whether they are mature MSPs or resellers transitioning their business models to managed services, are constantly refining their service delivery offerings. This requires the right balance of having a rich portfolio of services, but also the appropriate internal technology, processes and skills to deliver them.



2021

Number of partners

14,400
partners with managed services revenue in the 4 selected markets

3,700 4,350 3,650 2,700

MSP revenue: US$4.21 billion

MSP revenue growth: +9% in 2021

Source: Canalys estimates, Managed Services Analysis, October 2021

canalys

Cyber-resilience, such as that from Datto, allows partners to unify cybersecurity offerings in terms of the policy control, visibility and intelligence of their customers' IT organizations by centralizing software and appliances, whether they are on-cloud or on-premises. The "assume breach" mentality is the basis of becoming cyber resilient to attacks, and as the number of devices increases, the use of sound security principals can help grow and optimize operational efficiency and responsiveness while reducing costs and supporting partners' adoption of more mature cybersecurity services provisioning. Supporting the approach principals of cyber-resilience are five trends that demand further action to be taken to improve cybersecurity standards and resilience, both internally and for customers.

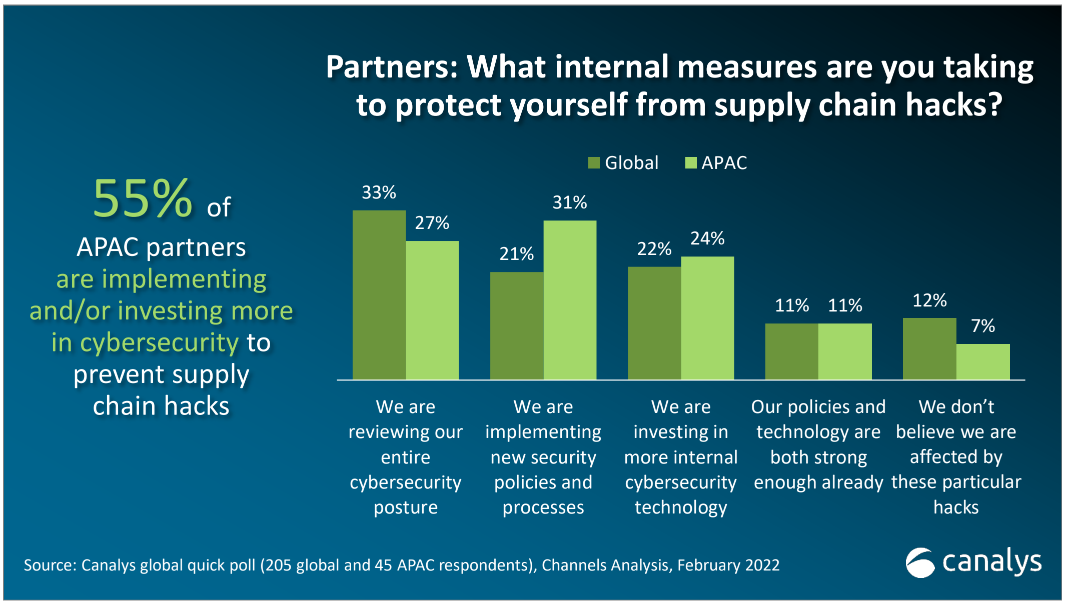
1. Malicious attackers are targeting MSPs and technology firms

MSPs have increasingly been targeted by malicious attackers over the last five years, especially ransomware operators, due to the huge volume of customer data they have access to. More are taking precautions to strengthen their own cybersecurity posture, such as conducting penetration tests and increasing employee training. Still, too often, MSPs are being targeted, with many still waiting until they become a victim of a cyber-attack before taking steps to address their cybersecurity policies.

MSPs, often with many disparate platforms and tools, as well as a broad range of customers, make ideal cyber-targets. MSPs have a multiplier effect that make them attractive targets for attackers to infiltrate and, once inside, push ransomware, change passwords, extract data or perform other malicious activities. An MSP that has access to large numbers of customers' data records will always be a target.

But in some cases, attacks are beyond their control, as highlighted by recent high-profile cases, such as the REvil ransomware attack in July that caused widespread downtime for over 1,000 companies, and the SolarWinds breach reported in December 2020, which allowed attackers to gain access to end-customer systems. Customers have no direct relationship with the attacker when MSPs are hacked and are not best placed to handle the attack.

Providing managed services in the ASEAN region can be difficult, as customers are sometimes unwilling to wholly trust their entire infrastructure and data to a third party, instead preferring a more collaborative approach. Earning trust is an ongoing mission. One way is to deploy the best cybersecurity practices.



Partners: What internal measures are you taking to protect yourself from supply chain hacks?

55% of APAC partners are implementing and/or investing more in cybersecurity to prevent supply chain hacks

Source: Canalys global quick poll (205 global and 45 APAC respondents), Channels Analysis, February 2022

2. Legal and financial consequences of non-compliance in cybersecurity, privacy and data sovereignty are intensifying

While the ASEAN region today has no single comprehensive legislation around MSPs, like the European Union, many governments are in the process of further strengthening cybersecurity regulations and standards. Customers expect their MSPs to be compliant and investing in backup and disaster recovery solutions can help in that regard. The shift is a positive for the region, in terms of driving greater awareness and stressing the importance of cybersecurity. MSPs can also play an active role in educating customers around these developments, and help choose the right cybersecurity solutions, as well as ensure legal needs are met and standards are improved. Existing laws in some ASEAN countries with high Internet penetration are already comprehensive around data protection and illegal data access, according to the Global Cybersecurity Index 2020, recently published by the United Nation's ITU. In the assessment carried out in 2020, countries that scored full marks under its "legal measures" category included Malaysia, Philippines, Singapore and Vietnam.

When implementing best practices around data protection, MSPs and customers should logically begin with the local data privacy and protection laws, which place the burden of protecting sensitive data on data controllers and processors. Even though most cyber-law penalties are designed to punish cyber-offenders, which include MSPs and customers, breached organizations also bear the brunt of the initial attack, including financial loss, reputational damage and disruption to business operations. These losses can affect an organization's credit ratings with banks, further affecting their cashflow. They can also affect credibility with suppliers and customers in terms of future business.

Key local cybersecurity-related laws and regulations

Singapore

- Singapore Cybersecurity Act
  - Adopts a light-touch approach toward the licensing of penetration testers and managed security operations center (SOC) monitoring service providers. Licenses valid for five years, renewable.
- Personal Data Protection Act
- Computer Misuse Act

Malaysia

- Computer Crimes Act
- Communications and Multimedia Act
- Personal Data Protection Act

Philippines

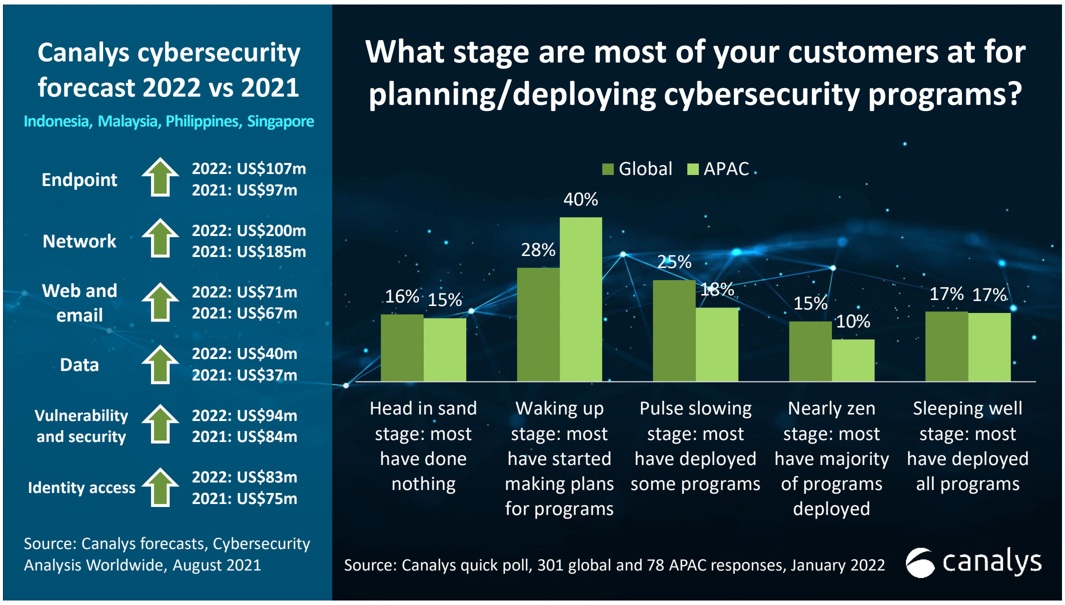
- Data Privacy Act
- Cybercrime Prevention Act
- Department of Information and Communications Technology (DICT) Cloud First Policy
  - Provides classifications for government data and guidelines around the access, storage, processing and transmission of government data in the cloud.
  - Also, provisions for ICT capacity building and development of essential skills to meet international and local standards.

Indonesia

- Electronic Information and Transactions Law
- Personal Data Protection in Electronic Systems regulation
- Implementation of Electronic System and Transaction regulation
  - Private electronic system operations (ESO), including MSPs, must register with MoCI.
  - Data localization requirements vary by type of ESO.
  - Organizations with "strategic electronic data" must connect electronic documents and backup records to a data center in the case where the incident must be reported to the cybersecurity authority.

3. Customers are driving suppliers and partners to be more cybersecurity compliant

High-profile supply chain attacks have exploited weaknesses in third parties as an initial entry point into their intended victims. Consequently, a growing number of organizations, especially large multinationals, are requiring their suppliers and business partners to pass cybersecurity tests. These requirements can be complicated and time consuming, such as answering risk assessment forms containing over 2,000 questions, submitting penetration testing reports, appointing a cybersecurity officer, and implementing ongoing awareness and education programs. MSPs are often seen as the CIOs of business customers in the small and medium-sized segments, and they in turn need to rely on trusted vendors to help build cyber-resilience and deliver peace of mind to their customers through secure business continuity and disaster recovery solutions, patch management and ransomware detection to mitigate the impact of attacks. Altogether, these show the growing cybersecurity emphasis in the ASEAN region.



Canalys cybersecurity forecast 2022 vs 2021

Indonesia, Malaysia, Philippines, Singapore

	2022	2021
Endpoint	2022: US$107m	2021: US$97m
Network	2022: US$200m	2021: US$185m
Web and email	2022: US$71m	2021: US$67m
Data	2022: US$40m	2021: US$37m
Vulnerability and security	2022: US$94m	2021: US$84m
Identity access	2022: US$83m	2021: US$75m

Source: Canalys forecasts, Cybersecurity Analysis Worldwide, August 2021

What stage are most of your customers at for planning/deploying cybersecurity programs?

Global
APAC
16%
15%
28%
40%
25%
18%
15%
10%
17%
17%
Head in sand stage: most have done nothing
Waking up stage: most have started making plans for programs
Pulse slowing stage: most have deployed some programs
Nearly zen stage: most have majority of programs deployed
Sleeping well stage: most have deployed all programs
canalys

Source: Canalys quick poll, 301 global and 78 APAC responses, January 2022

4. Cybersecurity insurance only protects companies that are cybersecurity compliant

The private cybersecurity insurance industry will drive positive changes in cybersecurity, but insurance should be an organization's last line of defense. Before buying cybersecurity insurance, customers are required to have an in-depth analysis of their business risks and exposure. Cybersecurity insurance transfers some financial risk to the insurer in exchange for a regular premium fee. But underwriters typically require clients to demonstrate a high standard in their cybersecurity posture, ensuring minimal losses are incurred for both customers and themselves.

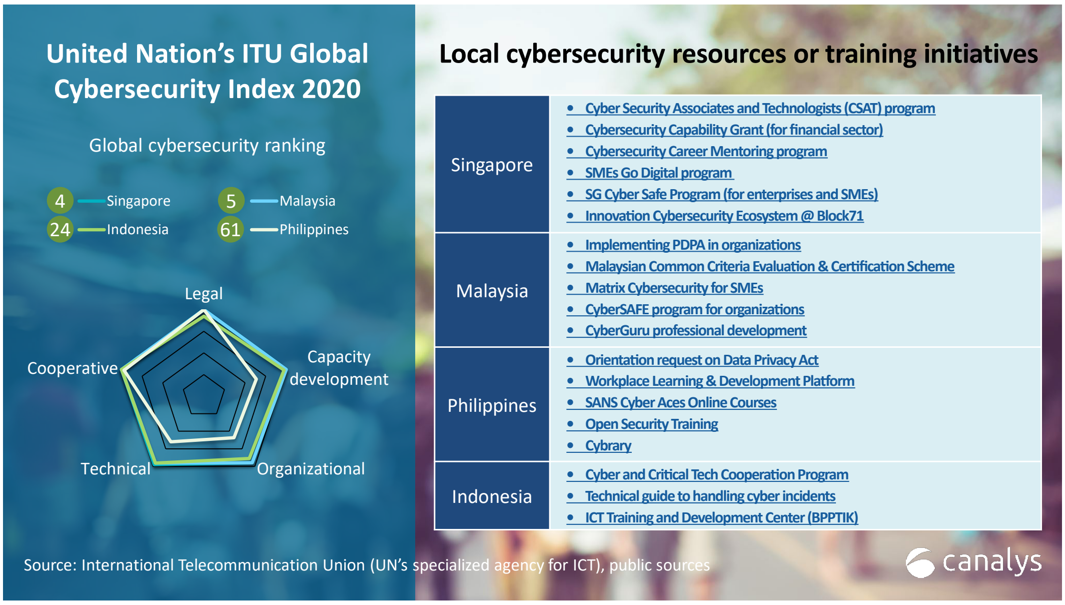
Generally, insurance reduces an organization's financial risk in the case of a data breach involving sensitive personal information, such as personal identity numbers, credit card accounts, and biometric and medical records. When organizations buy a comprehensive policy, the insurer will also cover costs and expenses resulting from data breaches that occur at outsourced independent companies managing the data. Costs and expenses from data breaches can come from, but are not limited, to the following:

- Privacy regulatory defense and penalties.
- Cyber-extortion, such as that from ransomware.
- Crisis management event.

- Loss and recovery of digital assets.
- Repair or replacement of computer systems.
- Business interruption expense.

5. Lack of internal cybersecurity skills

The lack of personnel with appropriate cybersecurity skills remains a major concern, not just for the ASEAN region, but worldwide. This affects the emphasis organizations place on cybersecurity education among their workforce internally, where human errors continue to be a leading cause of data breaches and other cybersecurity incidents. Even among IT professionals, it is hard to admit that complacency is often a key contributing factor. Online fraud, phishing and fake news are the most frequent incidents in Singapore, Malaysia, Philippines and Indonesia, and organizations must reinforce the importance of security hygiene and educate employees on telltale signs of suspicious content and scams. Not only do MSPs play a central role in cybersecurity, but governments also seek to boost awareness and build good cyber-hygiene habits across the population. Such campaigns are ongoing as part of coordinated national cybersecurity plans, and governments often offer cybersecurity kits or checklists that organizations can use.



United Nation's ITU Global Cybersecurity Index 2020

Global cybersecurity ranking

Local cybersecurity resources or training initiatives

Singapore	• Cyber Security Associates and Technologists (CSAT) program • Cybersecurity Capability Grant (for financial sector) • Cybersecurity Career Mentoring program • SMEs Go Digital program • SG Cyber Safe Program (for enterprises and SMEs) • Innovation Cybersecurity Ecosystem @ Block71
Malaysia	• Implementing PDPA in organizations • Malaysian Common Criteria Evaluation & Certification Scheme • Matrix Cybersecurity for SMEs • CyberSAFE program for organizations • CyberGuru professional development
Philippines	• Orientation request on Data Privacy Act • Workplace Learning & Development Platform • SANS Cyber Aces Online Courses • Open Security Training • Cybrary
Indonesia	• Cyber and Critical Tech Cooperation Program • Technical guide to handling cyber incidents • ICT Training and Development Center (BPPTIK)

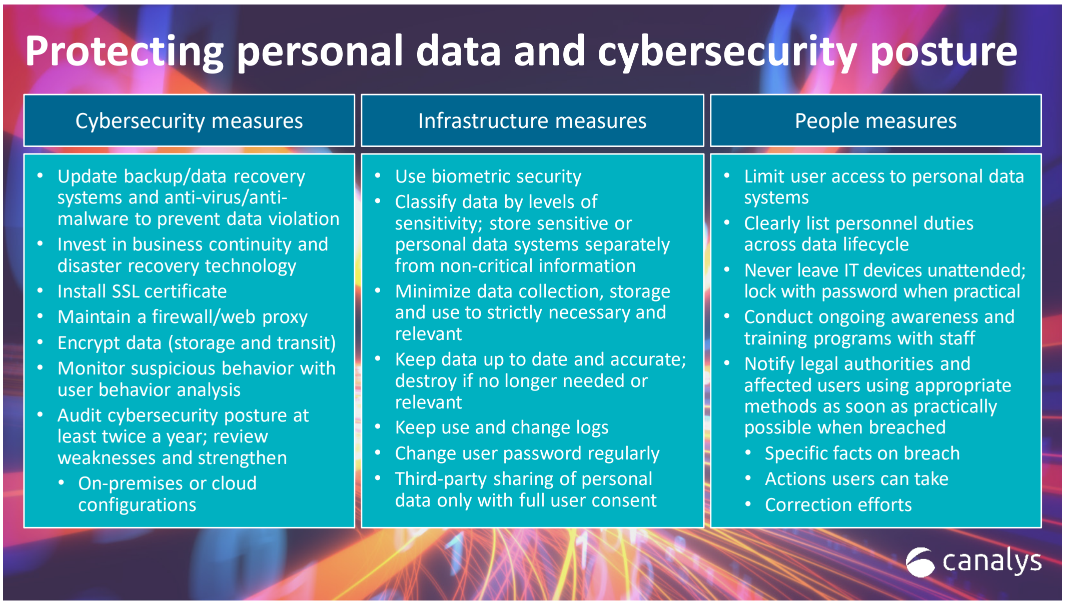
Source: International Telecommunication Union (UN's specialized agency for ICT), public sources

How can MSPs increase relevance to customers?

Many ASEAN MSPs are keen to develop cybersecurity and data management skills further to capitalize on customer demand. The range of different technologies that providers can use to support their service offerings is increasing, and it can often be confusing to decide where to begin. Here are a few specific practices that will help partners grow relevance and differentiation.

- **Proactively conduct cybersecurity training for employees and customers:** Moving beyond awareness and basic cyber-training requires a plan. Tabletop exercises came out as one of the most effective ways to improve business readiness, as suggested by cybersecurity researchers following the VSA breach suffered by a major MSP vendor. Many companies provide incident response plans and other methods to train for an incident. If this feels like closing the stable door after the horse has bolted, think of it more as acknowledging no door is impregnable, and you are developing ways to repair the door and get the horse back. Incident response plans will vary depending on the business but designating certain key individuals and training them in real world exercises is vital. Encouraging individuals to take on certain responsibilities can be useful and adopting a strong incident response framework can also be a way to improve service offerings to customers.

- **Invest in cybersecurity partner competencies:** One way MSPs can stand out from the competition is to earn cybersecurity partner competencies that they can use to promote their capabilities when they fulfill requirements, such as having certified individuals and reaching certain customer satisfaction scores. The cybersecurity market is growing, and a competency showcases an MSP's cybersecurity practice commitment and often rewards partners with additional benefits, such as marketing resources, training resources or financial incentives. MSPs can work with their partner account managers to create a plan to earn one or find out how they can get additional customer support from vendors. Many cybersecurity competencies are available today.



Protecting personal data and cybersecurity posture

Cybersecurity measures

- Update backup/data recovery systems and anti-virus/anti-malware to prevent data violation
- Invest in business continuity and disaster recovery technology
- Install SSL certificate
- Maintain a firewall/web proxy
- Encrypt data (storage and transit)
- Monitor suspicious behavior with user behavior analysis
- Audit cybersecurity posture at least twice a year; review weaknesses and strengthen
  - On-premises or cloud configurations

Infrastructure measures

- Use biometric security
- Classify data by levels of sensitivity; store sensitive or personal data systems separately from non-critical information
- Minimize data collection, storage and use to strictly necessary and relevant
- Keep data up to date and accurate; destroy if no longer needed or relevant
- Keep use and change logs
- Change user password regularly
- Third-party sharing of personal data only with full user consent

People measures

- Limit user access to personal data systems
- Clearly list personnel duties across data lifecycle
- Never leave IT devices unattended; lock with password when practical
- Conduct ongoing awareness and training programs with staff
- Notify legal authorities and affected users using appropriate methods as soon as practically possible when breached
  - Specific facts on breach
  - Actions users can take
  - Correction efforts

- **Emphasize customer communication:** Features such as multi-factor authentication may be tedious for customers, but they are necessary to prevent disastrous outcomes. Shake things up by conducting random phishing tests with employees. People are better served when they are personally informed through experience and customers can work with partners to build more comprehensive solutions to fit their digital business needs. That means understanding where their apps and data are held, how they are managed, and how they can be recovered in the event of an emergency or cyber-incident. Also ensure that customers know the lines of communication they have access to. MSP support teams must take steps to address customer concerns.

- **Audit remote admin tools:** One area often neglected is the auditing and testing of tools to discover potential flaws or weaknesses. Understandably, it is time-consuming and few MSPs have the internal resources to dedicate to testing. But, if possible, it is good to have some awareness at least of the possible ways a breach could happen when looking at your tech stack. For example, a common issue with RMM tools is IP address "whitelisting", which allows certain IP addresses to access networks. This can be seen as an effective security tool, keeping out threat actors if there are other properly configured tools in place, such as device identification or secure gateways to authenticate users. But without these measures, a whitelist is a potential threat. Whatever your access tools or policies, it is important to be aware of the security of your IT admin tools, even if you are unable to make changes, as it provides you with the right knowledge to assess alternatives.

- **Develop end-to-end solutions and services:** The questions channel partners must often answer when outlining data management solutions are around data privacy and sovereignty. Data must be secure and comply with local and industry regulations. It is important MSPs, whenever they can, develop end-to-end solutions for managing data, from the endpoint to the infrastructure, to the backup and recovery software and hardware and into the cloud. A more complete vision is vital for partners as they will have to show they are able to secure both on-premises and cloud applications and data.

- **Leverage a vendor's platform security and processes that are built into the solutions you wrap services around, from vendor management to cloud security:** Leveraging a vendor's inbuilt platform security is a fundamental step to improving one's security posture.

Looking ahead: selecting the right technology partner

An MSP cannot protect customers alone; providers require strong technology partnerships to give them the tools to monitor, manage and protect customers. Selecting the right set of technology partners is one of the most important things an MSP can do.

Today, over 17,000 partners around the world are turning to Datto's technologies to help deliver managed services solutions to over 1 million customers. While there are numerous reasons MSPs are selecting Datto, a few highlights stand out:

- **Datto offers SaaS-based solutions underpinned by a modern cloud infrastrucuture.** SaaS is increasingly becoming the model by which cybersecurity is delivered to customers. The benefits of this approach are numerous. Customers can rely on "always-on" protection from infrastructure designed to meet regulatory best practices that enterprises adhere to, and it ensures 99.99% uptime. Cloud encryption technology ensures customer data is protected, whether in transit or in storage. Meanwhile, the SaaS pricing model ensures customers can take comfort knowing their security costs are predictable.

- **Datto combines best-in-class cybersecurity protection with business continuity.** The reality is that no customer is 100% safe from a cybersecurity attack, and even large organizations that invest heavily in cybersecurity stacks can be breached. It is therefore paramount organizations not only have a cybersecurity strategy to reduce the risk from threats, but also a business continuity strategy should a successful attack occur. Datto provides detection, prevention, and flexible recovery that defends against costly downtime and data loss in servers, virtual machines and cloud applications.

- **Datto is designed, from the ground up, for multi-tenant environments.** There is an increasing emphasis across the technology community to develop solutions, programs and technology

> partnerships to support the MSP community. Increasingly, more vendors are coming to market with MSPs in mind. But only a few vendors are solely focused on MSPs, and dedicated to building solutions to help support those practices. Datto's secure offerings are designed for multi-tenant environments, meaning customers have their own protected instances, and MSPs can easily manage them via their own cloud-based administrative consoles. Through features such as mandatory two-factor authentication, and a geographically dispersed infrastructure, MSPs can lean on Datto to build their resiliency against cyber-events.

There are numerous opportunities for MSPs in the ASEAN region, but modern providers will need modern solutions. Threat actors have become more sophisticated and successful with their attacks, and traditional cybersecurity architectures and practices, widely deployed over the last 10 to 20 years are no longer flexible and scalable enough in this new paradigm. MSPs with the right technologies in their arsenal will be in an advantageous position as they look to help their customers navigate an increasingly threat-laden digital landscape.

datto

This report was commissioned by Datto

The written content of this document represents our interpretation and analysis of information generally available to the public or released by responsible individuals in the subject companies but is not guaranteed as to accuracy or completeness. It does not contain information provided to us in confidence by the industry. Market data contained in this document represents Canalys' best estimates based on the information available to it at the time of publication.

If you wish to use any information from this report in a public forum then you must receive prior explicit written approval from Canalys.