SPONSORED BY:

Red Hat | intel

C-SUITE SURVEY

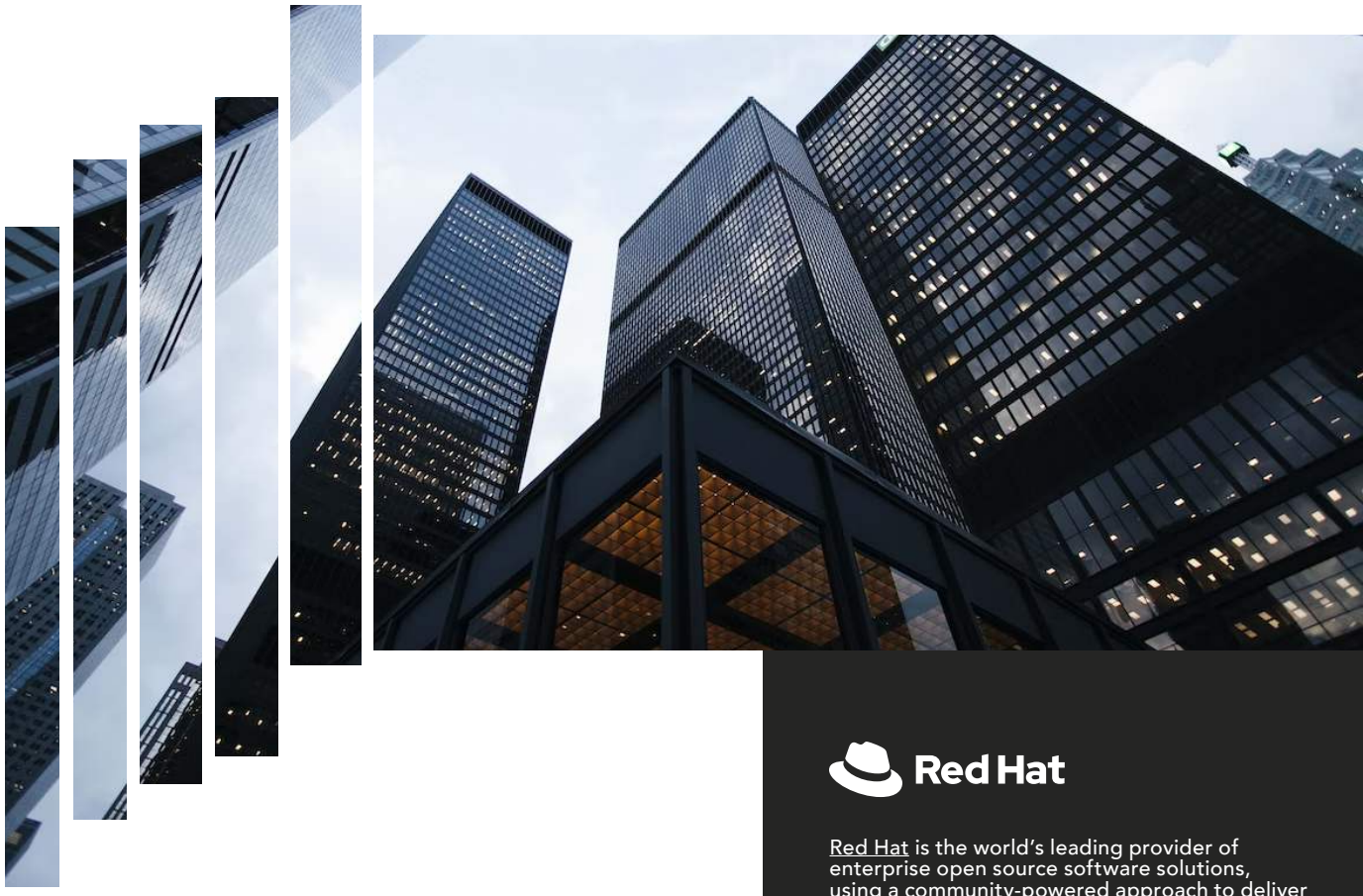
CYBER SECURITY READINESS IN ASIA PACIFIC

powered by:

FUTURECIO
Leading Enterprise Transformations

cxociety

CONTENTS



Red Hat

Red Hat is the world's leading provider of enterprise open source software solutions, using a community-powered approach to deliver reliable and high-performing Linux, hybrid cloud, container, and Kubernetes technologies. Red Hat helps customers integrate new and existing IT applications, develop cloud-native applications, standardize on our industry-leading operating system, and automate, secure, and manage complex environments. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500. As a strategic partner to cloud providers, system integrators, application vendors, customers, and open source communities, Red Hat can help organizations prepare for the digital future.

intel

Intel (Nasdaq: INTC) is an industry leader, creating world-changing technology that enables global progress and enriches lives. Inspired by Moore's Law, we continuously work to advance the design and manufacturing of semiconductors to help address our customers' greatest challenges. By embedding intelligence in the cloud, network, edge and every kind of computing device, we unleash the potential of data to transform business and society for the better. To learn more about Intel's innovations, go to newsroom.intel.com and intel.com.

FUTURECIO
Leading Enterprise Transformations

FutureCIO is about enabling the CIO, his team, the leadership and the enterprise through shared expertise, know-how and experience - through a community of shared interests and goals. It is also about discovering unknown best practices that will help realize new business models. For more information, visit www.futurecio.tech

Introduction

We've come to realise that disruption and uncertainty are the hallmarks not only of the previous two years, but 2022 as well. For many financial institutions looking to modernise their operations in Asia, the pandemic has certainly accelerated their digital strategies.
But this connecting with customers digitally has also attracted the attention of cybercriminal elements. And while financial institutions have long been at the forefront of securing the customers' finances and data, they have done so from behind well-established protocols, practices and infrastructure that are secure-by-design.

This time around, the digital economy which is an ecosystem of different players connecting to an open platform, means end-to-end security may be not guaranteed 100% of the time.

It is with this in mind that CXOCIETY Research in partnership with Red Hat, surveyed 100 senior technology, security, and operations leaders to get their perspective on how the financial services industry across the key markets of Indonesia, Malaysia, the Philippines, and Singapore, are approaching cybersecurity preparedness as part of the business' digital transformation journey.

We hope that you find the insights that follow as helpful as you fortify your organisation's cybersecurity practice.

Methodology

Country representation
- Indonesia
- Malaysia
- Philippines
- Singapore

Target audience
Cybersecurity is the responsibility of all. While the Chief Information Security Officer, in partnership with the Chief Information Officer, may have responsibility for the overall strategy, the success comes from bringing together different practices within IT, security and operations to frame a holistic approach. In this regard, CXOCIETY purposely identified executives with different roles at financial institutions ranging from IT, security, risk management, infrastructure, and data management, to ensure broad representation of interest, experience, and expertise.

The study focused on three questions:
- How would you describe your organization's main cybersecurity approach?
- What is your organization's biggest security concern in its digital transformation?
- What is your top priority in terms of cybersecurity spending for the next 12 months?

Time frame
The survey was conducted from April to June 2022

Quantitative
The data was compiled and analysed, and the results used to frame questions and observations used as part of this document.

Qualitative analysis
At Cxociety, we recognise that when it comes to something as important as cybersecurity, data alone is not sufficient. A roundtable discussion was conducted in 24 June 2022 to provide context to the data and round out the analysis.

Rethinking cybersecurity amid digital transformation

Financial institutions need to adjust their cybersecurity baseline as they revisit existing security policies and processes after years on a digital journey.

Banks and other financial institutions have always been a magnet for cybercriminals out to make a hefty payday by perpetuating various online scams such as money laundering, credit card fraud and personal data leak to name a few.

In Southeast Asia alone, several high-profile banking hacks have drawn significant negative publicity in the past 12 months, jeopardising the industry-wide push toward digital banking.

Early this year in Singapore, customers of DBS and POSB **saw unauthorised withdrawals of thousands of dollars from their accounts due to a "click-free" phishing scam**. Likewise, during the same period, OCBC customers also reported **losing as much as S$100,000 – with some seeing their savings wiped out** – by an SMS scam that asked them to click on a link to prevent being locked out of their accounts.

In the Philippines, **700 BDO bank accounts were hacked before Christmas last year**, with an undisclosed amount illegally transferred to fictitious accounts at Union Bank. Unlike previous incidents, victims did not click on phishing links or unwittingly gave away their OTP data. Investigations made by the country's central bank revealed that the **hacking originated from a compromised web service**.

Indonesia's central bank itself **was targeted by cybercriminals with a ransomware attack last December**, but Bank Indonesia was able to implement mitigating measures to foil the attempt. No data leak occurred, and no public services were disrupted. DarkTracer, a platform that monitors and traces malicious activities online, said that Bank Indonesia was on a target list of cybercriminals using a malicious software dubbed "Conti".

According to the latest **Fitch report** released in June, the increased digitalisation of the financial sector across the region amid the COVID-19 pandemic raises the risk of cyberattacks that could cause reputational damage and affect the banks' viability ratings.

"Banks across APAC have been digitalising their service offerings at varying paces and the imperative to do so was accelerated during the COVID-19 pandemic when service channels overwhelmingly moved online. Faster adoption of digital banking presents new business opportunities and banks that managed the transition well have reinforced their business profiles compared with competitors," the report said.

"However, increased digitalisation also amplifies the technology-related operational risks that banks face and can expose them to reputational damage that weighs on their franchises. Cases of technological failure in APAC since 2016 have shown the potential to transform into wider financial risks that have an adverse impact on bank ratings," it added.

With technology today playing an essential role in facilitating banking services and providing the digital tools necessary for interaction between customers, employees, and other stakeholders, it is imperative for industry players to re-examine their cybersecurity posture to ensure protection against potential threats without hampering seamless business operations.

To determine the cybersecurity readiness of financial services companies in the region, Red Hat and Intel initiated a three-part survey that polled senior technology and security executives across five countries in Southeast Asia – Indonesia, Malaysia, the Philippines, Singapore, and Thailand.

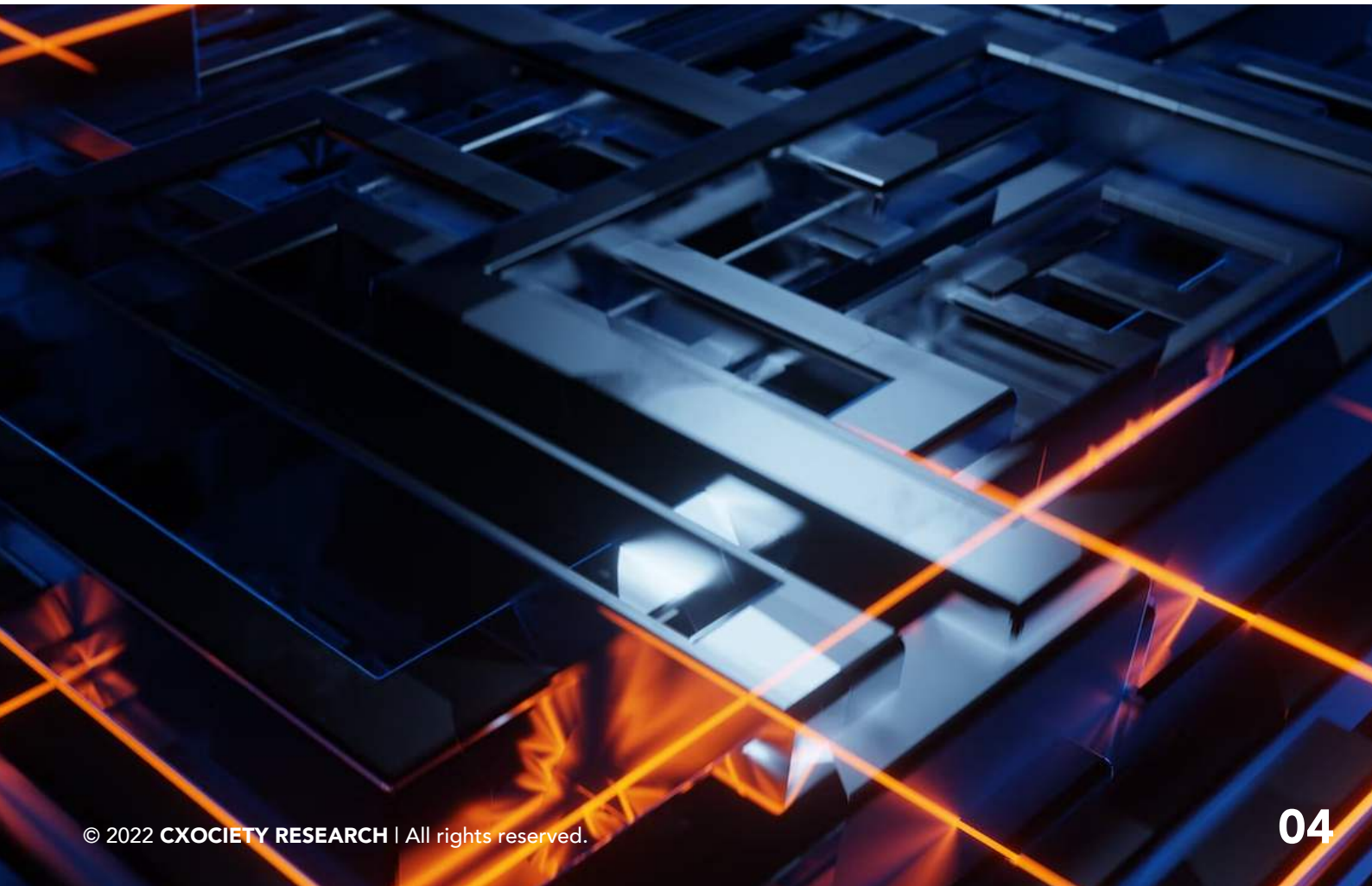
> ***"Hybrid is the predominant strategy with most organisations, and it makes sense because you want to have the best of both worlds,"*** ***- Christopher Tan, APJ INTEL***

The survey, conducted by FutureCIO, was unveiled recently in a virtual roundtable dubbed "Rethinking cybersecurity to support your digital transformation". FSI executives, who head their firms' technology and cybersecurity operations, joined the event to share additional insights into the questions raised in the online poll. All participants also came from the five countries included in the survey.

The majority of the participants have the challenge of securing the hybrid IT infrastructure in their respective organisation as computing resources and digital assets reside on-prem and in the cloud.

"Hybrid is the predominant strategy with most organisations, and it makes sense because you want to have the best of both worlds," said Christopher Tan, global partner revenue acceleration director, APJ at Intel.

"You want to have the flexibility, the agility, the cost benefits of cloud; but at the same time, there are some parts of your IT infrastructure – your data and your applications – that you still want to keep on-prem for many reasons from security, privacy to data sovereignty".



Choosing the right cybersecurity approach

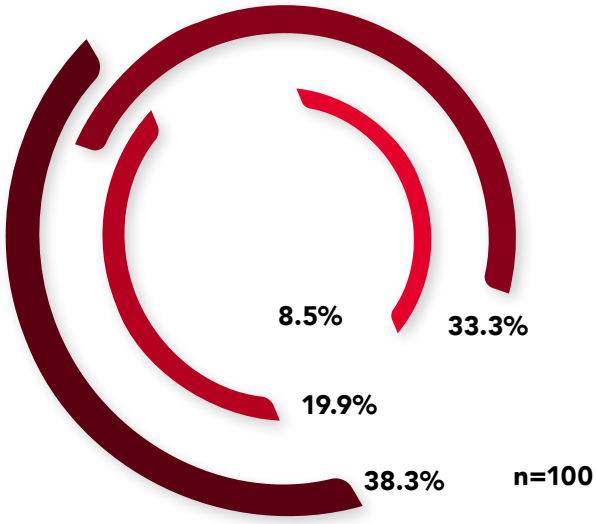
A majority, comprising 38%, of survey responses, claim to deploy monitoring tools to detect and mitigate cyberattacks. Among the countries included in the survey, the Philippines outpaces its peers in this category, followed by Singapore in the second spot. India and Malaysia both ranked third, closely followed by Thailand.

This predominant use of monitoring tools reflects the reality on the ground. With the expanding threat surface as well as the growing sophistication and frequency of security incidents, protecting an organisation from both external and internal risks has been an uphill battle. Cybersecurity as a round-the-clock task can only be managed effectively through automated monitoring to complement an overextended workforce, particularly amid the acute shortage of IT security professionals.

Twenty per cent (20%) of responses put the cybersecurity burden on external partners – relying on software and cloud providers – to secure their organisation's applications and data; while 9% said to adopt the ad-hoc approach of detecting and patching security holes and vulnerabilities as they found them.

Figure 1

How would you describe your organization's main cybersecurity approach ?



- We rely on monitoring tools to detect and mitigate cyber attacks
- Security by design; security is baked into every application from development to deployment
- We detect and patch security holes and vulnerabilities as we find them
- Our software and cloud vendors are responsible for ensuring our applications/data are secured

CXOCIETY RESEARCH SURVEY OF CYBER SECURITY READINESS IN ASIA PACIFIC 2022

What's interesting is that close to 33% of the total responses noted their financial institutions have put into practice the security by design principle, where security is built into every application from development to deployment. The figure is nearly as much as – only five percentage points from – the percentage of responses (38%) that say they rely on monitoring tools to detect and mitigate cyberattacks.

The survey results show that banks across the five countries are starting to have a more expansive view of cybersecurity and have taken a multi-pronged approach to protect their applications and data. Nearly a quarter (25%) of respondents are using two or more cybersecurity measures listed in the survey. From this figure, the Philippines and Singapore came out on top in having a well-rounded cybersecurity approach with 36% respectively, followed by Malaysia with 12%, while Indonesia and Thailand each have 8%,

At the roundtable, the majority of participants agree that banks need to forge several cybersecurity measures together into one holistic approach to safeguard their digital assets.

"As a security professional, there are three things you have to do: identify your security principles – that's where security by design comes into play; then, you deploy monitoring tools to detect potential threats; and once a vulnerability is discovered, you have to make a fast corrective action by patching the security hole," said a Singapore-based participant who is vice president for IT for a multinational bank.

Image by Lukas on Pexels

Survey results show, however, that banks in the region still need a nudge to broaden their cybersecurity posture, as 75% of respondents say their organisation only has one approach for guarding against potential threats. Of this number, 24% have placed the responsibility of securing their organisation in the hands of their cloud and software providers.

"CISOs always talk about it's a shared responsibility. But basically, it is their company's assets, and they still must be responsible for that. You can't ship that out to someone else to take responsibility with," said Tan of Intel. "I think all CISOs understand that while you can ship out your data – or maybe some of your application services – to a cloud provider, data security resides remains with you as the owner of the data."

Image by Our-team on Freepik

Among respondents whose respective companies have taken only one cybersecurity approach, it is notable that 39% picked using monitoring tools as their preferred mode of protection while 36% have adapted security by design, building security into their organisation's software development, as their sole method of defence against cyberattacks. These echo the overall results of the survey, where there is a very narrow gap between those who preferred one cybersecurity over the other.

One participant at the roundtable pointed out banks that keep 40-year-old legacy technologies alongside newer systems must deploy a blended cybersecurity strategy to secure two separate sets of business processes, which run in parallel.

"We operate a bimodal model. We have our mainframes on one side, and on the other side, we have our mobile banking site where Kubernetes is used for software development and deployment. It's two different technologies and we have split teams to manage these systems. We straddle between two worlds and there is a different cybersecurity approach for each one. We have built a big bucket of budget on monitoring for both worlds," he said.

Cybersecurity as a business enabler

Vincent Caldeira, chief financial services technologist at Red Hat, observed that financial institutions in the past invested in security technology from a control and regulation standpoint – and normally done as an afterthought.

> ***The cybersecurity paradigm has been turned on its head as the industry openly embraces the DevSecOps concept with the increased adoption of cloud and other digital technologies.***
> - Vincent Caldeira

"DevSecOps is about building a culture of collaboration between different teams and different functions in terms of how security is approached. This means that people such as developers and software engineers need to become more familiar with the security process and with the security controls that must be put in place. These people are critical in building a lot of these controls very early in the software engineering process and software deployment. Developers gain more knowledge of operations and security by contributing to this improvement," said Caldeira.

He also stressed that the bank's operations team must evolve as well by trying to understand the entire software supply chain – and how it potentially leads to automated deployment and easier monitoring when they deliver software.

"Now, security has become an enabler of better DevOps. Organisations have started to understand that if you do not build security into your process and you wait for the last minute to perform security checks, chances are your software is not going to end up in production – and you are not going to be able to have a very quick cadence of software release and deployment," said Caldeira.

"This whole drive towards more digital delivery has actually started to fuel investment in talents, in processes and in better security," he added.

He noted financial institutions that are successful at cybersecurity do not have problems with implementing monitoring tools.

"In fact, their problem is they have too many tools and we are trying to reduce them to make things simpler, Caldeira said, adding the major challenge is that every team in financial institutions has their own cybersecurity tools and each team does not understand the other teams within the organisation.

Caldeira revealed a significant work that Red Hat does from the software development process is around security – specifically helping companies adopt a unified enterprise automation capability.

"This means reducing the number of different monitoring tools that companies use for detection. We try to integrate the tools a lot more, and obviously, we try to converge all technologies around security automation – that different teams can use whether you're talking about the network team or the development team," he said.

Customer data leakage is a prime concern

Embracing the security by design principle is no guarantee that financial institutions are 100% from internal and external threats, according to one roundtable participant.

"Even if the bank has been very serious on security by design – meaning every application we develop has first gone through a series of security screening and architectural screening to make sure the technology we use and deploy satisfy the banking standard in terms of cybersecurity, there are always new applications in the public cloud that may not be secure from a banking business perspective; and, users may not be aware of them," said the participant, who handles machine learning engineering at an international bank.

He noted: "Sometimes [even a very tight control mechanism] cannot cover every loophole. There could be things especially when we're talking about cloud journey /cloud migration, so it's very difficult to cover all aspects of security when we are dealing with a vast pool of technology from the cloud providers."

He also points out that the threats usually come from users who are not aware of what they are doing, a sentiment shared by virtually all his peers at the roundtable.

Furthermore, all of them agreed that customer data leakage caused by the lack of employee compliance with security policies is the number one cybersecurity concern in their organisation's digital transformation.

Senior bank officials who were polled in the FutureCIO survey showed the same fear occupying the top spot of their organisation's security concern. Survey results showed 33% of total responses have customer data leakage due to employees' lack of compliance as the number one cybersecurity headache among the countries polled – except in Thailand where the top spot was the inability to detect and respond quickly to external threats.

In ranking the banking industry's cybersecurity concerns, the survey also revealed that unknown threats and vulnerabilities in their internal network take the second place with 22% of responses, followed by unsecured devices/systems accessing the corporate network with 17% of responses, the inability to detect and respond quickly to external threats get 15% of responses, while employees clicking phishing emails garnered 13% of responses.

A roundtable attendee stressed that organisations need to revisit all their basic hygiene controls.

"People think these controls are working, but they are not optimised to work effectively. Simple things like patch management – we realised that there are a lot of gaps to cover after going through years of digital transformation," he said.

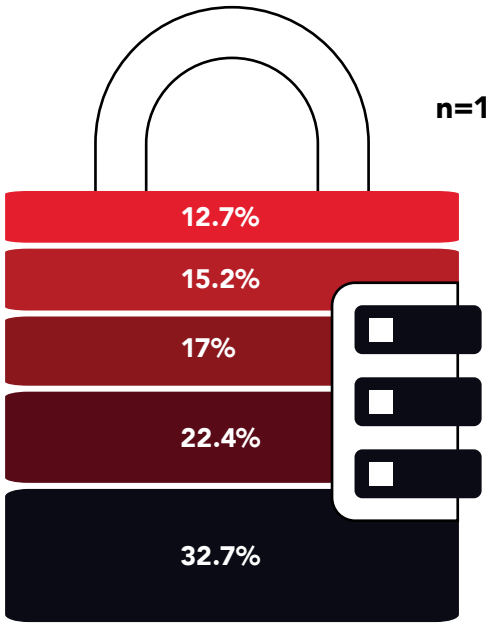


Figure 2

What is your organization's biggest security concern in its digital transformation?

- Customer data leakage due to lack of employee compliance with security policies
- Unknown threats and vulnerabilities in your internal network
- Unsecured device/systems accessing the corporate network
- Inability to detect and respond quickly to external cyber threats/attacks
- Employees clicking on phishing email and/or misconfiguration error

CXOCIETY RESEARCH SURVEY OF CYBER SECURITY READINESS IN ASIA PACIFIC 2022

Protecting data with security by design

Tan of Intel said financial institutions can adopt the security by design principle to protect their systems from leaking data to threat actors.

"Today, hackers attack you from an application level, from an OS level, from a VM level. There's no way we can protect that 100%, so we try to make it harder for them to break in by creating a secure enclave within the CPU on the hardware platform," Tan said.

As an example, he cited Intel's Xeon platform which has the SGX technology that allows an organisation to build security even at a deeper level of the infrastructure.

"It makes it more difficult for hackers to break in and the use case for SGX is really for you to be able to mask the data when it's in process," Tan explained.

At present, organisations can encrypt their data while in motion and when they are being stored. The only time data are vulnerable is when they are being processed.

"With SGX, we now create a secure enclave within the platform where this data will be processed and it can only be seen at a very high-security level, which makes it not visible to the OS. the firmware or even the applications.

"The use case here is that if you can do that, you can secure your keys at that level and process the data so you're processing the data without seeing the data. Conceptually, it means that you'll be able to then share data in what we call a federated use case," said Tan.

This is very important for the FSI industry, he pointed out.

"If you want to detect fraud, if you want to detect money laundering, you need to be able to run your AI algorithms across institutions not just within your institution. And today that's very difficult to do because everybody's worried about sharing their data."

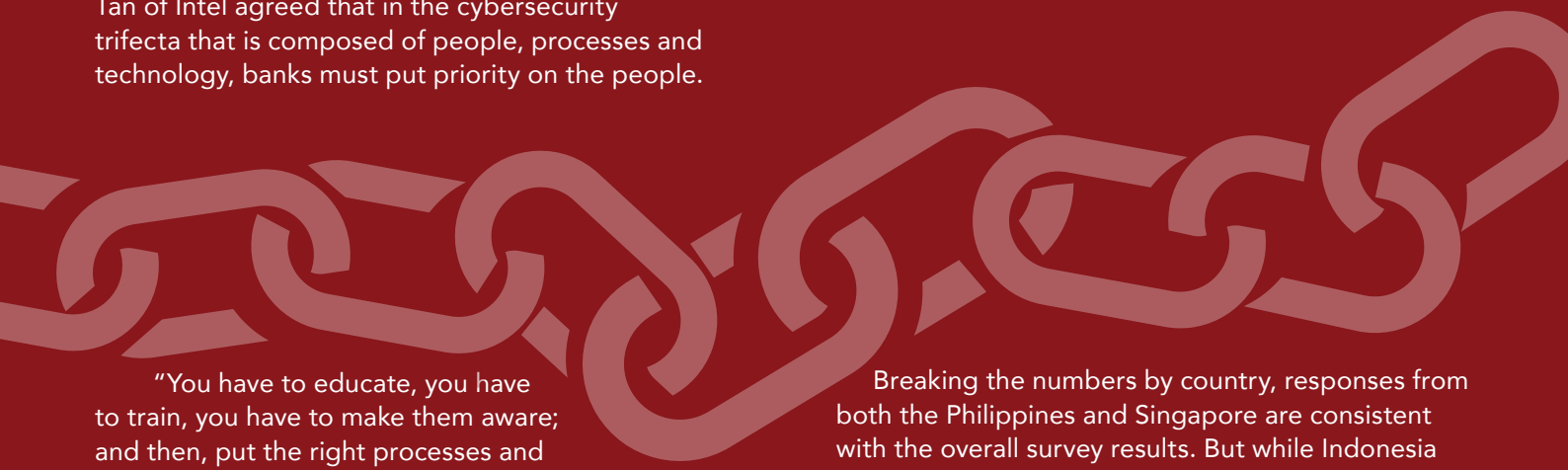
"But with SGX, it's possible for you to then share data in that sense without actually seeing the data. So, you see the results of your AI algorithms, but you don't necessarily see the data. Federated learning is something that is becoming a very strong use case in what we call regulated industries like banking healthcare and so on. This is one of the areas that we want our customers to look at," said Tan.

People are the weakest link

Meanwhile, participants at the roundtable identified the weakest link in the organisation's cybersecurity posture, which was not included in the survey options: people.

> ***"We spend a lot of effort on user education and awareness of simple things like phishing and not capturing things on your screen. We can control the machines but it's the user we can't control,"*** an attendee said.

Tan of Intel agreed that in the cybersecurity trifecta that is composed of people, processes and technology, banks must put priority on the people.



"You have to educate, you have to train, you have to make them aware; and then, put the right processes and policies in place to ensure your cybersecurity, then the technology comes in. As we push into digital transformation, we must be ready for this, or we are exposing ourselves to a lot of threats," said Tan

Unsurprisingly, several participants at the roundtable felt it is imperative for organisations to embark on a culture change that would put security awareness into the very core of the corporate structure.

"We are currently engaging all our end users, cultivating security awareness as part of the corporate culture within the enterprise," said one roundtable attendee.

Another attendee said a security-aware corporate culture is necessary because organisations have to continuously overhaul and review existing policy processes to keep the pace of digitisation, shifting business priorities and changes in regulatory requirements.

For this culture change to happen, they are advocating for regular user training that provides the dos and don'ts to keep computing resources and digital assets safe.

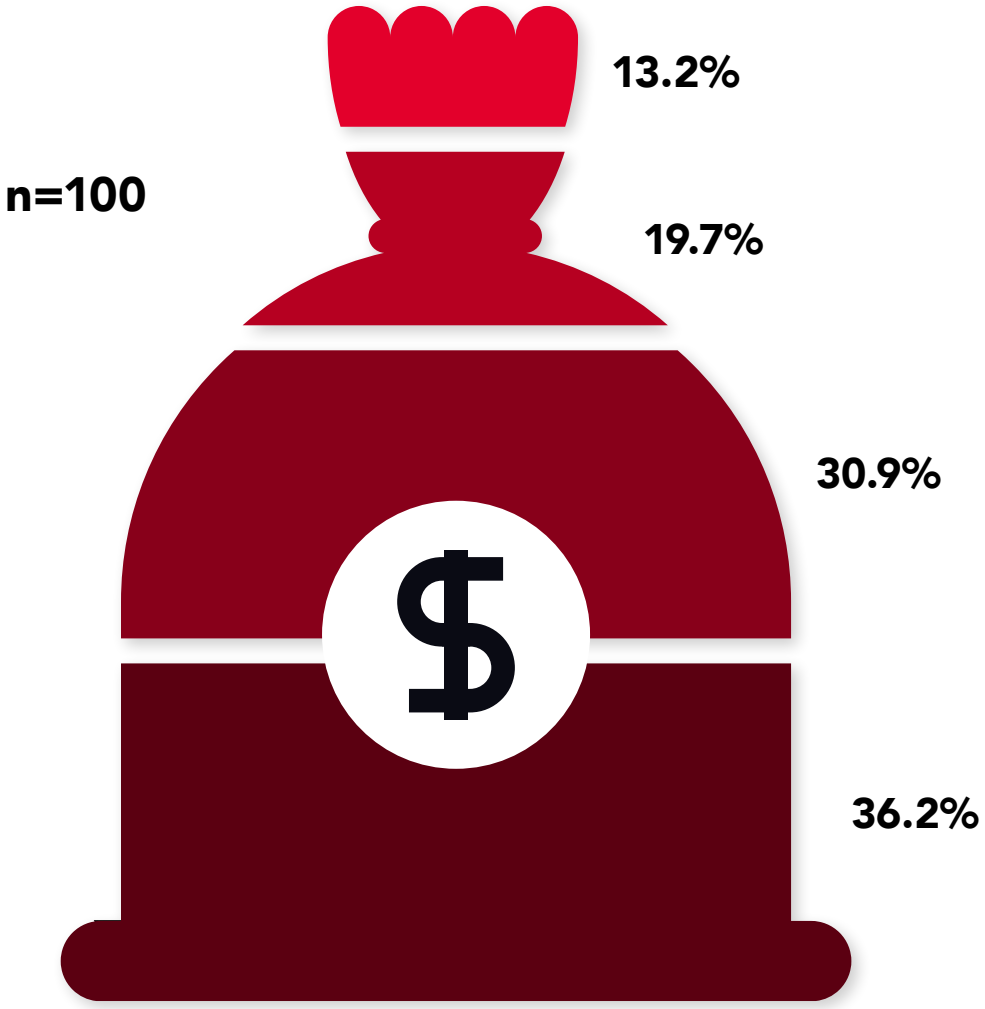
Banking industry insiders polled in the FutureCIO survey have placed cultivating a security-aware corporate culture through user education and training as the top priority in the next 12 months in terms of security spending, garnering 36% of total responses. The next priority item in their purchase list is the automation of security monitoring and detection tools, which got 33% of responses. Meanwhile, 20% of respondents want to put part of their annual cybersecurity spending on AI-powered security monitoring and 13% of respondents want to earmark some budget on new hires to expand the security team.

Breaking the numbers by country, responses from both the Philippines and Singapore are consistent with the overall survey results. But while Indonesia similarly placed cultivating a security-aware corporate culture (42%) on top on its spending priority in the next 12 months, the country's senior banking officials have the expansion of their security team (26%) with new hires as the second item on their cybersecurity budget; followed closely by automation of security monitoring and detection (21%); and AI-powered security tools (11%).

Malaysia has automation of security monitoring and detection tools as the first item on its cybersecurity budget list at 38%; with AI-powered security monitoring at 29%; cultivating a security-aware corporate culture at 19% and hiring security team members at 14%. Like Malaysia, Thailand puts automation of security monitoring and detection tools on the priority list at 42%. This is followed by cultivating a security-aware corporate culture at 33%; expanding security with new hires at 17%; and AI-powered security monitoring at 8%.

Figure 3

What is your top priority in terms of cybersecurity spending for the next 12 months?



- Cultivate security-aware corporate culture through user education and training
- Automation of security monitoring and detection tools
- Artificial Intelligence-powered security monitoring
- New hires to expand cybersecurity team

CXOCIETY RESEARCH SURVEY OF CYBER SECURITY READINESS IN ASIA PACIFIC 2022

Automation is the way to the future

Overall survey results clearly showed that deploying automation of security monitoring and detection tools is top of mind among the polled senior banking executives. The cultivation of a security-aware culture may have gotten 36% of responses – and can be seen as a strategic approach – but automation gained as many responses with just a three percentage points gap at 33%, which suggests respondents feel that it is a primary tactical measure for protecting their organisation's digital assets moving forward.

Participants at the roundtable clearly have automation as a major part of their security toolbox in the next 12 months and beyond.

"The proliferation of online attacks such through SMS scams makes security monitoring and detection key to our cybersecurity roadmap. Also, with digital banks coming on board, there will be less human automation so automation will play a bigger role," said one attendee.

Another echoed: "Automation is an important way that can eliminate some of the human errors because if most of the things are handled by reliable technology and systems, then people have fewer touch points to be doing things that can be used to the enterprise."

A third participant pointed out that with limited resources, financial institutions must turn to automation. "We make use of whatever technologies are available. But ultimately, we need to understand the threat that we are facing and then use those threats to align the automation efforts."

Caldeira of Red Hat observed while organisations focused on automation, they should also balance this with investment in people.

"We just won't have enough people out there to do the entire job of handling security, so definitely automation is also going to be a big theme of investment. However, automation without people is useless, but people without automation is also going to be a very big challenge going forward because if you look at the typical footprint of an organisation in adopting potentially multiple public clouds, the complexity of running security has increased tremendously," said Caldeira.

He also stressed the importance of the use of open-source technology and open security design across the organisation to achieve implementation of security control – particularly as many organisations are in early-stage adoption of cloud technology, and cloud-native capability.

"They need to rethink the entire security baseline that they built over the years to consider the emergence of cloud. I truly believe in the principle of open design. A lot of the emerging trends around it involve the adoption of infrastructure as code, and compliance as code – which basically make compliance policy, and security policy a lot more open. Managing source code that can be looked at by more pair of eyes with more humans in the process to actually improve the security procedure of the organisation," he added.

Re-evaluate security practices and strategies

The risk of security breach and attacks increases exponentially as financial institutions start to open up and share data across different parties (internal or external third party providers) within the ecosystem.

To ensure the safety of data and other digital assets, industry regulators have been setting the benchmark with mandates and guidelines that require banks and financial institutions to implement security best practice, particularly in an open hybrid cloud setup

Red Hat said: "As organisations look to their digital transformation initiatives, they should adopt security best practices like Zero Trust, Security by Design etc, to secure their infrastructure and data against different attack vectors internally and/or externally, regardless of whether they are on-premise at the organisation's location, in a hosting environment or in the public cloud. These best practices should also be employed to all users in the ecosystems regardless whether they are internal employees, administrators or end users like customers."

To gain compliance and a good reputation of being a safe and secure organisation to work with, organisations need to re-evaluate their security practices and strategies as they look to transform their business, processes and offerings to their customers.

For more details about securing your digital assets in the public cloud, click here.

CXOCIETY PTE LTD
531A Upper Cross Street #04-95
Singapore 051531
www.cxociety.com
Email: publishers@cxociety.com