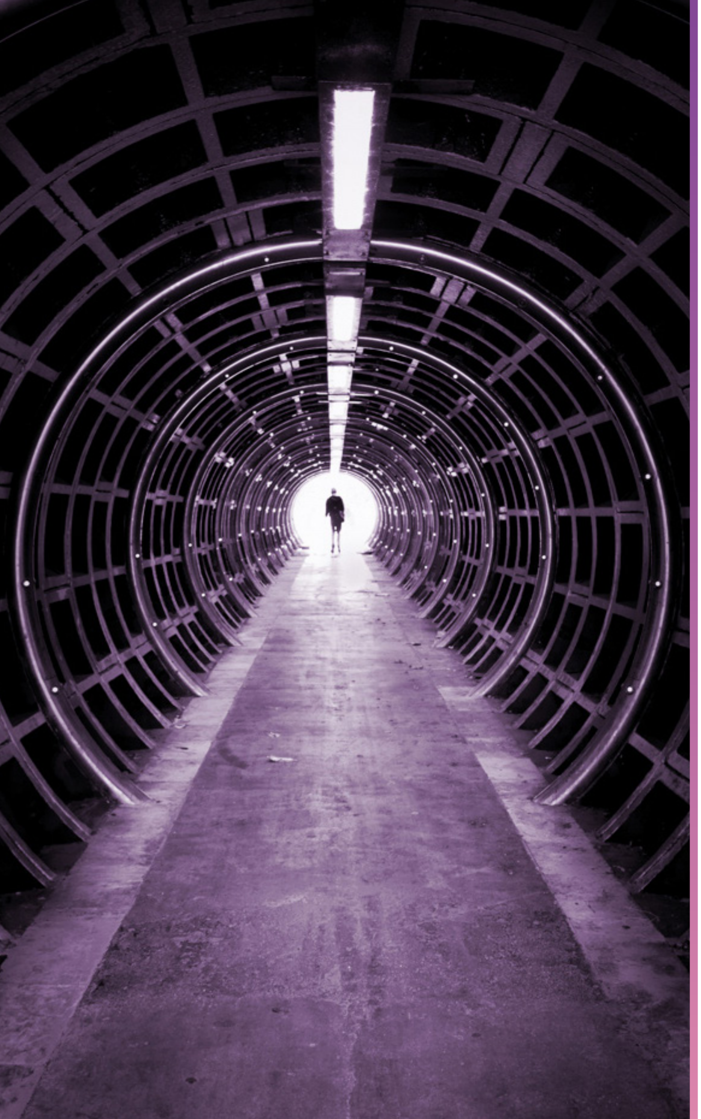


THE STATE OF DATA READINESS

CYBER RESILIENCY EDITION

ASEAN

February 2024

A Tech Research Asia Insights Report,
commissioned by Commvault.

INTRODUCTION

Welcome to our 1st edition of The State of Data Readiness in ASEAN

We all know ASEAN companies are facing complex data and cyber environments. It's tough and unrelenting.

Executive business leaders want 'always on' access to the data and systems that underpin business operations.

Tolerance of technology outages is low and business executives have high expectations about how quickly a company can come back online if attacked.

Technology experts also know that the recovery reality is somewhat different. When it comes to how quickly an organisation can recover after an attack, it's not a matter of being operational in hours or days, it's typically weeks or months.

This gap between expectations and reality has pushed cyber resiliency higher up executive agendas. Organisations are looking to create or strengthen their ability to continue business operations and deliver outcomes even when experiencing cyber attacks and to accelerate their ability to recover if breached.

This report provides data and commentary on:

- **Data growth, current data infrastructure in use, and the prevalence of dark data;**
- **The top 2 issues impeding data management & security;**
- **Breach recovery expectations and realities and the factors that influence these;**
- **Cyber attacks;**
- **AI usage in cyber, data recovery rates, and breach awareness; and**
- **The importance of partners.**

We hope that you find value in comparing your organisation to your ASEAN peers, and that the insights in the report help you to enhance and strengthen your own data management, recovery, and cyber resiliency capabilities.

Sincerely,

Tech Research Asia

The data provided in this Commvault commissioned TRA Insights Report comes from 900 companies in Indonesia, Malaysia, The Philippines, Singapore, Thailand, and Vietnam. Additional information on this sample can be found in the appendix of the report.

HIGHLIGHTS FROM THIS REPORT

- There is a significant disconnect between business expectations and technology reality when it comes to restoring business operations if breached.
- The research data shows that companies are not recovering all their data, nor can they maintain business operations when breached.
- There is an inevitability to being breached and cyber resiliency is critical.
- Threat actors target a mixture of data environments, increasingly looking at production + secondary + backup estates as a ‘nuclear’ option.
- Cyber resiliency maturity is low and organisations continue building and enhancing their capabilities.
- Immutability, cleanrooms, AI and partners can help bolster Cyber Resiliency effectiveness.

DATA ESTATES

Growth, dark data, and infrastructure

We don't expect data growth to slow in the coming 12 months.

ASEAN companies experienced average growth in their data estates of 31% in the last 12 months. Of that growth, our analysis suggests 60% was unstructured data (i.e. data that is difficult to store in a traditional database format), requiring significantly more management to be optimised and transformed into value.

With companies accelerating their adoption of artificial intelligence (AI) solutions such as generative AI, the subsequent content creation will fuel increases in the amount of data retained, as well increasing the proportion of data that is unstructured.

However, with organisations looking to reduce or at least optimise their costs, there is a clear focus on data storage optimisation and eliminating 'no-value, low-value' data. Those organisations that managed to reduce their data estates saw an average reduction of between 6-8%.

With data estates continuing to expand in the high majority of organisations, the research shows 61% of ASEAN companies are following a blended 'best-fit' approach spanning public and private clouds and on-premises infrastructure to support their data. Another 13% are solely on-premises and 14% are using a single public cloud environment.

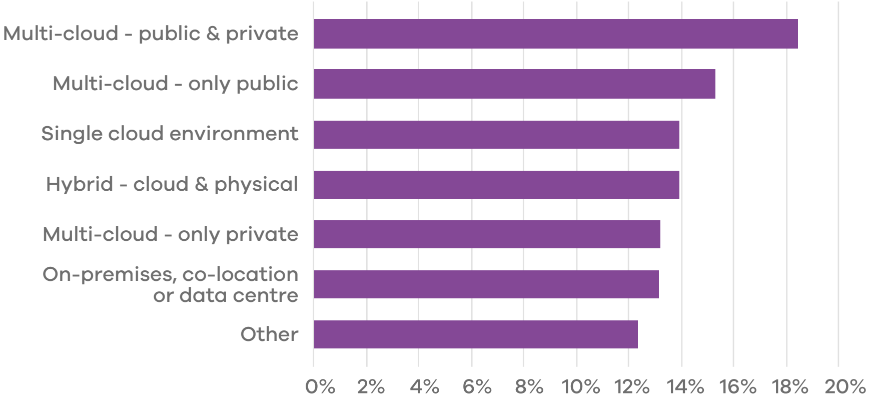
The scalability and flexibility of cloud brings advantages, however it also means companies can quickly create copies of data sets, or entirely new data sets, that can reside outside of conventional data management, security, and recovery solutions.

This data and infrastructure sprawl also contributes to dark data (i.e. data that is created and unmanaged or sits outside of the businesses' scope of management control and/or visibility).

By its very nature, dark data is difficult to manage, and in many cases, organisations may be unaware exactly how much dark data they have and where it resides. In ASEAN, 91% of companies state they have challenges managing dark data.

> *"The moment a company can standardise on an integrated recovery platform, it has a better shot at being able to control, manage, govern, remediate, and recover."*
>
> **Michel Borst**
> Area Vice President for Asia, Commvault

"Thinking about the data your company currently stores and manages, please estimate the percentage of data stored in each of the following locations."



THE TOP 2 ISSUES IMPEDING DATA MANAGEMENT & SECURITY

Recoverability, we have a problem...

Alongside data/infrastructure sprawl and dark data, the top 2 operational challenges organisations cited in managing and securing their data environments are:

1. **Effective and speedy data recovery after a breach; and**
2. **Establishing a robust cyber resiliency capability.**

Let's dig a little more deeply into these 2 issues, starting with data recovery after a breach.

Business expectations for recovery time don't align with technology reality

Our research reveals a substantial disconnect between the time business leaders expect to be 'up and running' after a breach or attack and the time IT professionals require for recovery.

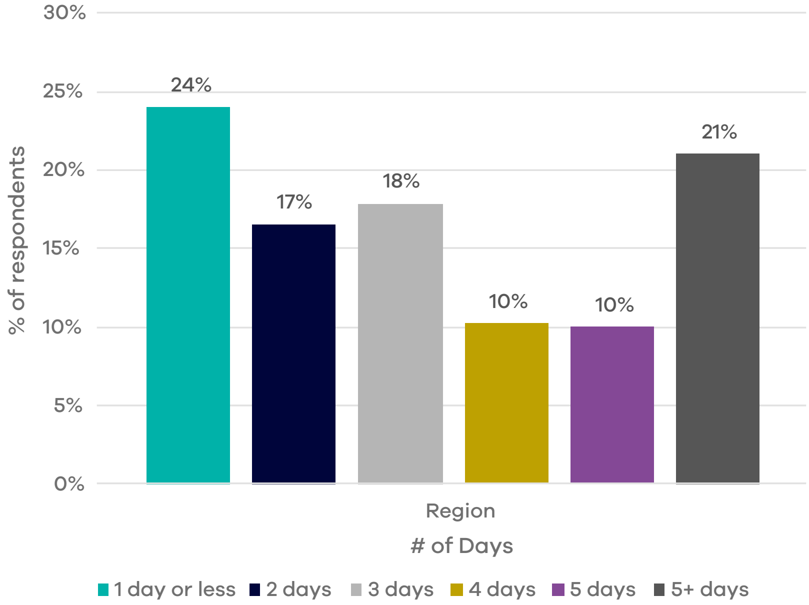
For business leaders, speed of business resumption is the critical factor – 24% of leaders say an outage of 1 day or less is tolerable and by the end of day 5, 79% of leaders expect the organisation to have data access restored and be back in business.

Let's be clear, 79% of business leaders want to be back in business after a cyber incident in **5 days or less.**

The average time IT professionals in our research reported it took to recover from a breach? **4 to 5 weeks.**

Plainly, there's a problem between business expectations and IT reality.

From your perspective as an executive business leader, how long could your business tolerate an outage with restricted access to critical data?



BREACH RECOVERY

3 Things Business Executives Need to Consider

The 5 days to 5 weeks difference is challenging, and it helps to understand some of the common issues our research revealed that contribute to the complexity of recovery, namely:

1. **It's not just 'one thing' that gets targeted in an attack – recovery spans production, secondary, and backup environments;**
2. **The 'cloud' brings benefits but also has limitations; and**
3. **Just because a company has an incident response plan doesn't mean it works.**

Have you been attacked?

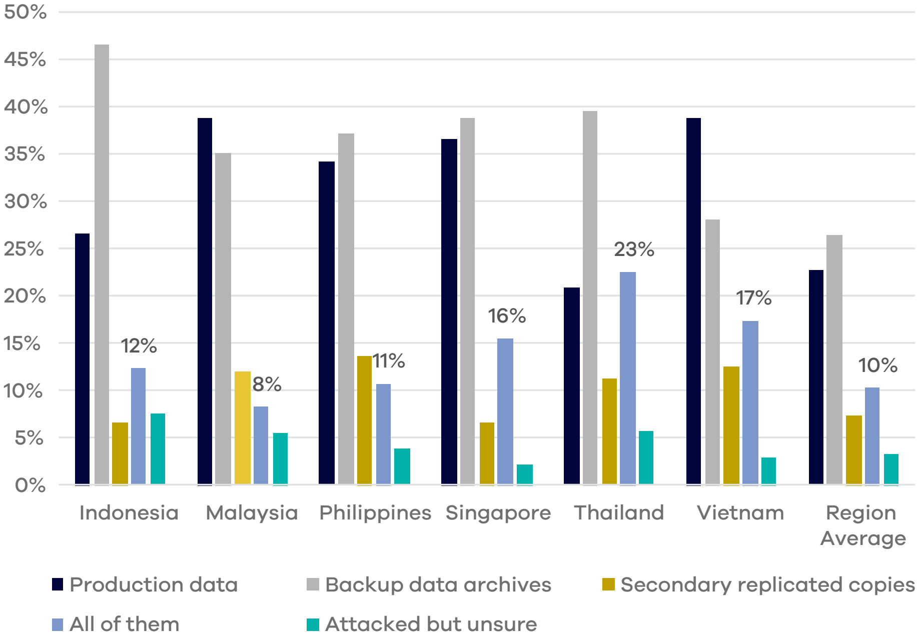
On average, 71% of companies stated they had been subjected to at least one cyber attack in the last 12 months, with more companies in Thailand (83%) and Malaysia (72%) experiencing above average attacks, and companies in Singapore less (60%).

These attacks do not simply target one part of the infrastructure that supports business operations, for example, just the production environment. Increasingly, attacks are multi-faceted, targeting 2 or more areas such as production and back-up, or production and secondary, and, in 10% of companies attacked, the 'nuclear option' of all 3 environments – production, secondary and back-up.

Attacks on all 3 environments were highest in in Thailand (23% of attacks), Vietnam (17%) and Singapore (16%), with attacks on production data highest in Malaysia, Vietnam (both 39%), and Singapore (37%).

Thinking about the most recent cyber attack your company experienced, did it target…?

(Note: Multiple responses allowed, totals exceed 100%)



> *"For companies to be truly prepared for an incident, it's not just IT and security that need to be ready. It needs these groups, business owners, and lines of business heads to work closely together…"*
>
> **Michel Borst**
> Area Vice President for Asia, Commvault

BREACH RECOVERY

Cloud – it's both good and bad

Having a blended, multi-infrastructure environment provides flexibility and scalability.

In fact, 85% of respondents indicated they are either using, or intend to use cloud services in the next 12 months, to manage and secure their multi-infrastructure environments.

The potential problem here is that using cloud native tools (e.g. Azure tools for Azure, AWS for AWS, GCP for GCP, etc.) can create inefficiencies.

Each tool is optimised for its own infrastructure. This makes it difficult to create a standardised data management platform that works effectively across multiple environments. Extending further into physical, on-premises as well as cloud only exacerbates the issue.

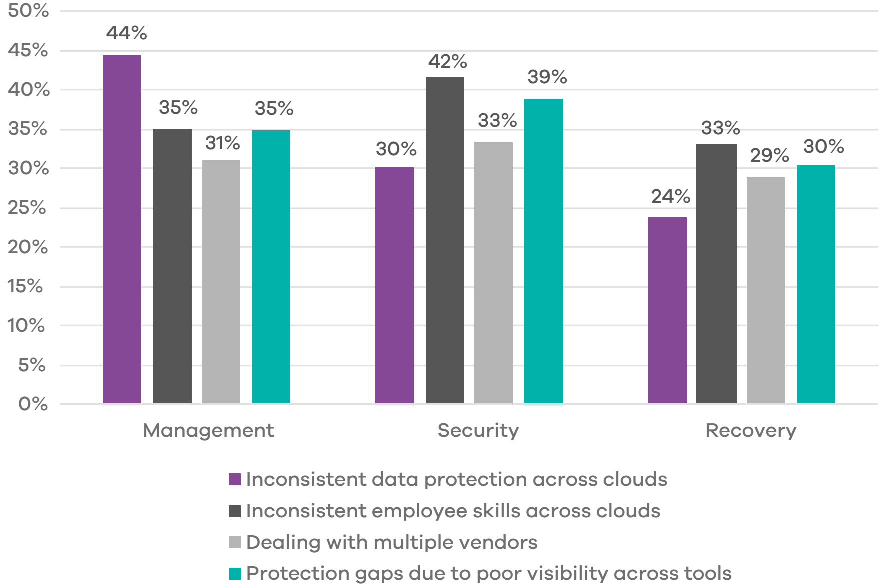
Looking across the research data reveals that:

- **44% of companies experience inconsistent data protection management across different clouds.**
- **This can lead to problems in managing, securing and recovering data for 1/3 of companies due to inconsistent employee skills between different cloud and on-premises environments, and**
- **At least 30% of companies suffer from poor visibility across disparate tool sets leading to gaps in their ability to manage, secure, and recover data.**

In these circumstances, variable data protection capabilities across environments increase the pressure on businesses to have consistent skills to address each appropriately.

This, compounded with having to engage with multiple vendors, creates a lack of visibility into, and gaps in, recovery capabilities, ultimately costing organisations more in terms of costs and time to recover.

What are the top challenges you face using native data management, security and recovery tools in a multi-infrastructure environment?



BREACH RECOVERY

You have an incident response plan. But when did you properly test it?

On average, 85% of companies surveyed stated they have an incident response plan that is used to support their response and recovery activities if attacked.

So why is it when asked about the effectiveness of their company's incident response, only 26% responded that "There is a clearly understood response and communication plan in place, roles are clearly understood and we perform very well."?

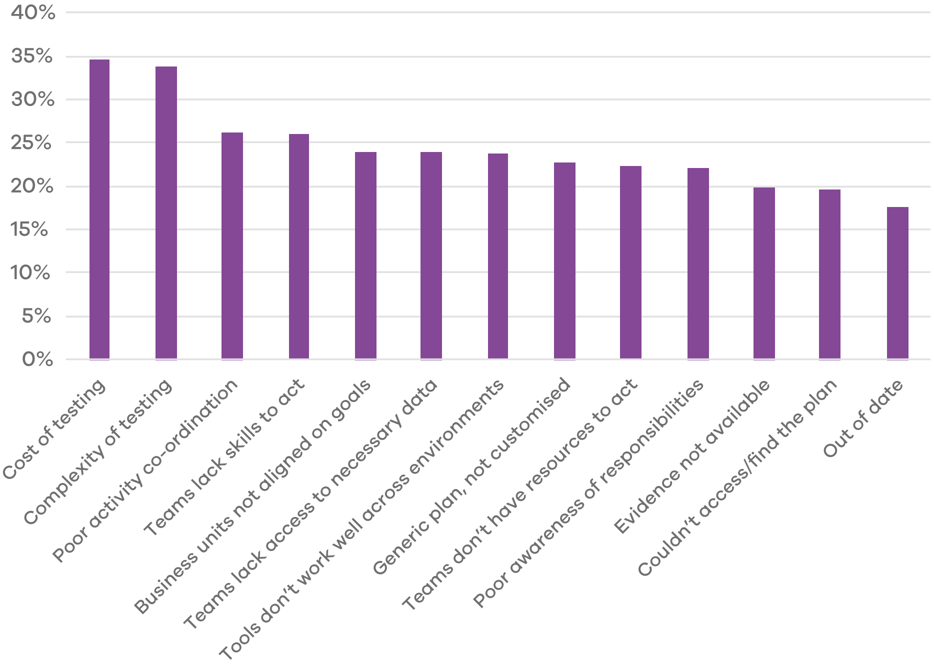
Of the remaining respondents, 22% stated their incident response capability "...is very unorganised and we scramble to respond. Our response is poor."

Active testing is very different to a 'table-top' review. Our research revealed several problems that make companies reluctant to vigorously test their plans including:

- **Cost;**
- **Complexity;**
- **Lack of planning activity and co-ordination;**
- **Teams not having the right skills to act on testing the plan; and**
- **Business incident response plan objectives are misaligned with IT objectives.**

Troublingly, 20% of companies stated they couldn't find or access the plan to test it, despite having one prepared.

What prevents you from properly testing your incident response plan?



CYBER ATTACKS

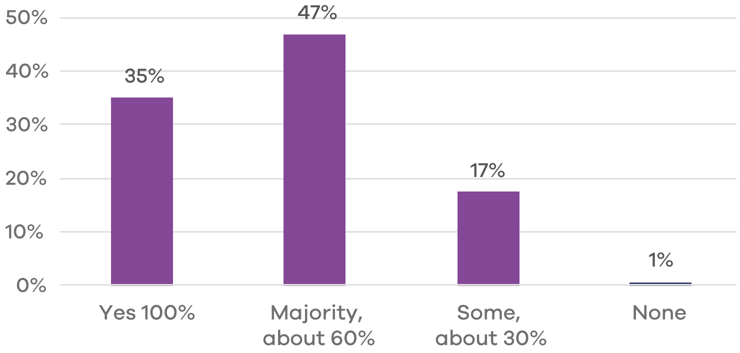
Data recovery rates & breach awareness

As mentioned earlier, 71% of companies experienced at least one cyber attack in the last 12 months. Did the companies attacked recover all their data?

Not quite. Only 35% stated they successfully recovered 100% of their data.

Businesses need to move beyond 'are backup jobs running?' to a more proactive stance to ensure compromised data is 100% recoverable and have solutions like data clean rooms and immutability in place to support this.

You stated your company was targeted in a ransomware attack and suffered a data breach or loss. Did you completely recover your data?

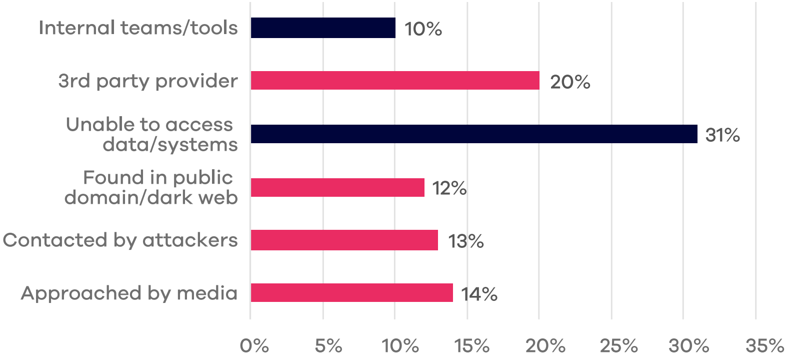


How did companies discover they had been breached?

Unfortunately, the most common way companies discovered they had been breached was through events external to their operation.

- 59% of companies found out because they were informed by their 3rd party security provider, approached by media (14%), contacted by attackers (13%), or found their data in the public domain or dark web (12%).
- 31% became aware when they were unable to access their data or systems; and
- 10% from their internal teams or security tools.

When did your company first become aware it had been the subject of a data breach or loss?



CYBER SECURITY = CYBER RESILIENCY

Not really.

Let's explore the 2nd issue organisations identified that has a direct impact on effective and speedy business recovery – cyber resiliency.

Isn't cyber resiliency the same as cyber security?

No. Cyber security concentrates on creating and maintaining an overall approach that protects digital assets.

The National Institute of Standards and Technology (NIST) defines cyber security as "The ability to protect or defend … from cyber attacks". Broadly, it focuses on prevention via tools such as firewalls, encryption and antivirus, with the aim of addressing threats (internal and external) to prevent breaches and unauthorised access.

Resiliency has a number of key differences, starting with the NIST definition: "The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources[1]."

As such, cyber resiliency focuses on adaptability and recoverability, through strong incident response plans, backup and recovery systems, and incorporates business continuity, risk management and training. Rather than prevention, resiliency focuses on continuity even if breached, assuming that attacks and breaches are inevitable.

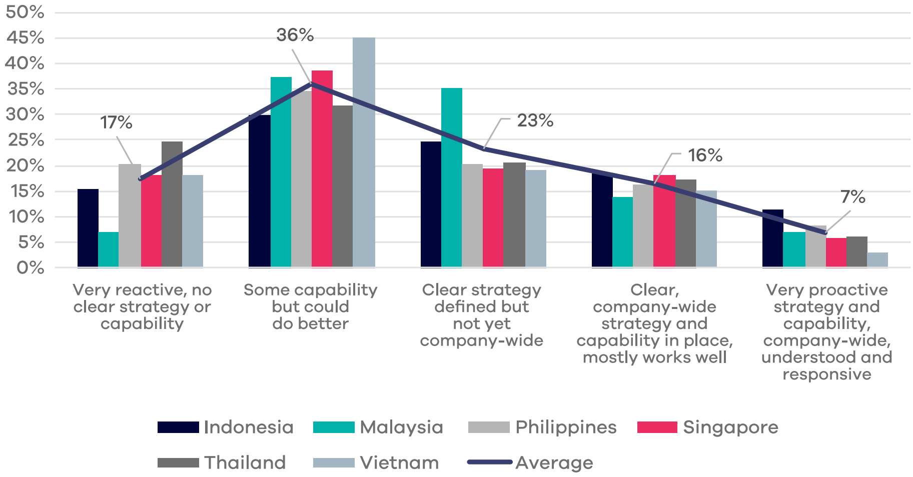
How mature are ASEAN companies when it comes to cyber resiliency?

Cyber resiliency clearly has a critical influence on maintaining business operations. Our data suggests many companies are in the early days of establishing strong cyber resiliency strategies and capabilities.

Only 7% of companies in the region believe they have a 'proactive, mature cyber resiliency capability'. Another 16% consider their business to have a capability that 'mostly works well'.

Of the remainder, 17% have 'no strategy or capability', 36% 'could do better,' and 23% 'have clarity but lack a company-wide strategy'.

Thinking about cyber resiliency, which of the following statements best describes your company's maturity level?



[1] Source: https://csrc.nist.gov/glossary

STRENGTHENING RECOVERY AND RESILIENCY

Some quick wins to bolster capability

As part of this research, we asked organisations what other investments or initiatives are considered important to recovery and improving cyber resiliency. Four key areas were identified:

1. **Data immutability.** Increasingly important for organisations seeking cyber risk insurance, having an immutable copy of data provides for quicker recovery, better data integrity and compliance, and more effective auditing and forensic capabilities. However, maintaining immutable data across multi-infrastructure environments that doesn't impact system performance and increase data management complexity was identified as the top challenge for organisations when trying to secure their data estates.

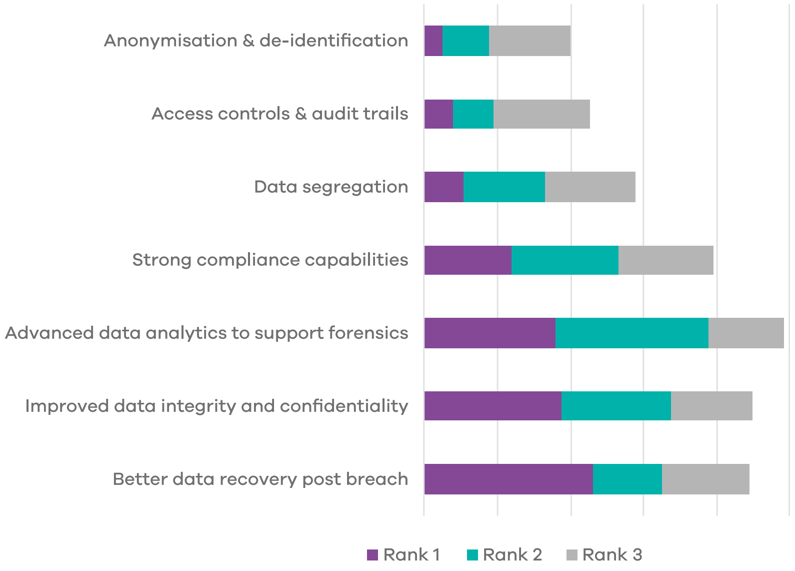
2. **Data cleanrooms.** 92% of companies are using data cleanrooms across the region, highlighting some key advantages they bring to their recovery and resiliency stances:

   - Better data recovery post breach ranked #1 by 28% of respondents;
   - Improved data integrity and confidentiality ranked #1 by 23% of respondents; and
   - Advanced analytics support forensics ranked #1 by 22% of respondents

3. The adoption of **artificial intelligence** for cyber security.

4. Using **partners** to enhance skills and response capabilities.

Please rank the top 3 benefits your company gets from using data cleanrooms where 1 is 1st benefit, 2 = 2nd, etc.



> *"Testing incident response and cyber readiness plans isn't easy but it is critical. The trouble is that it can be cost-prohibitive with significant disruption to the operations. Testing in cleanrooms is a great way to avoid these problems whilst validating forensic operations."*
>
> **Michel Borst**
> Area Vice President for Asia, Commvault

AI FOR CYBER SECURITY AND RESILIENCY

Offensive or defensive AI, or both?

The third area identified in our research the adoption of AI solutions to strengthen cyber capabilities.

Much has been written about the growth of generative and other artificial intelligence solutions in the cyber and broader technology arenas. We're not going to add to that here.

Rather, we wanted to explore if companies were adopting AI for cyber security and if so, was the focus more offensive or defensive in intent?

We learnt that 74% of companies are either using AI, or plan to use in the immediate future to support their cyber security and resiliency.

Within the region, Indonesia, The Philippines and Thailand showed highest levels of usage/intent and Malaysia, Singapore and Vietnam showed lower levels of adoption and intent.

Of those using AI:

41%

are using AI defensively, with firewall management the most popular defensive application (46% deploying);

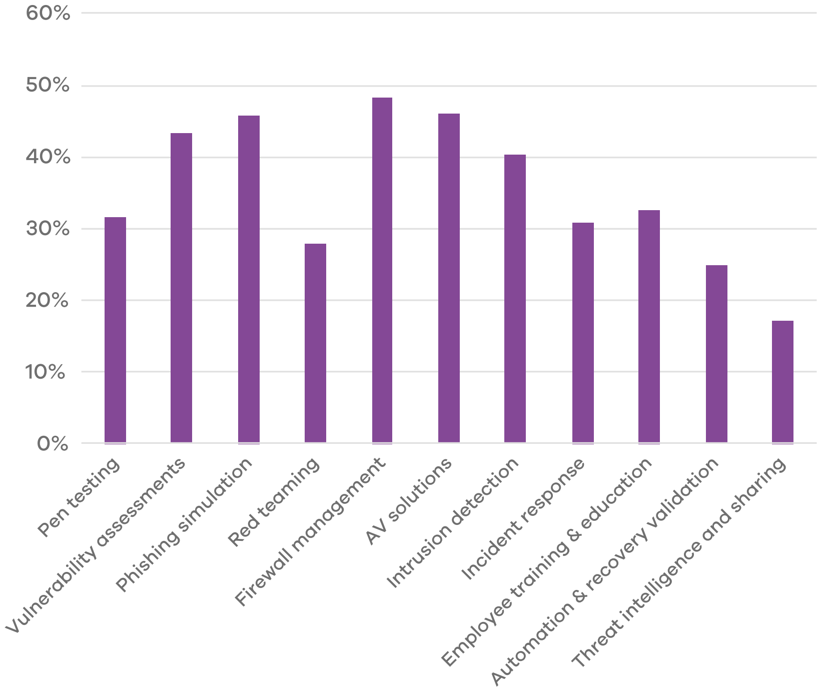
36%

are using it offensively with phishing simulation being the most popular application; and

23%

are using it for both offensive and defensive purposes.

Where do you use AI tools in your cyber security and data protection environments?



> *"We're already seeing strong interest in AI from companies in ASEAN. The uses cases are comprehensive including classifying, indexing and analysing data estates, ensuring data segmentation across securely governed domains, as well as automation and orchestration."*
>
> **Michel Borst**
> Area Vice President for Asia,
> Commvault

PARTNER ECOSYSTEM SUPPORT

Enhancing capabilities and lifting skills

More than 80% of companies in region engage technology partners to support data management, security, and recovery operations.

Partners were identified as bringing a range of advantages and capabilities with the top 5 being:

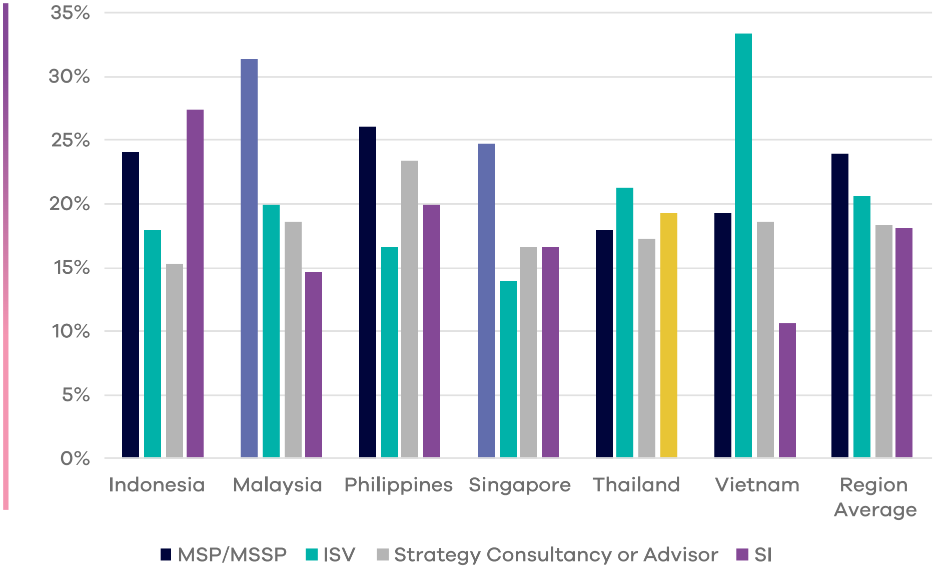
1. **Skills availability;**
2. **Infrastructure, cyber operations (and related vendor) management;**
3. **Breach recovery and incident analysis;**
4. **Education and training; and**
5. **Management of governance, risk, and compliance requirements.**

The preferred type of partner by country varies considerably and can be seen in the table:

Indonesia	Malaysia	Philippines	Singapore	Thailand	Vietnam
SI	MSP/MSSP	MSP/MSSP	MSP/MSSP	ISV	ISV
MSP/MSSP	ISV	Strategy consultancy	Strategy consultancy	SI	MSP/MSSP
ISV	Strategy consultancy	SI	SI	MSP/MSSP	Strategy consultancy
Strategy consultancy	SI	ISV	ISV	Strategy consultancy	SI

Legend:
MSP: Managed Service Provider
MSSP: Managed Security Service Provider
ISV: Independent Software Vendor
SI: Systems Integrator

What type of technology partner is your preferred choice for your company's data management and cyber security initiatives? (Top 4 partner types only shown)



IN CLOSING

We sincerely hope you found value in the report and the analysis helps you when considering your recovery and resiliency capabilities.

For many organisations, data growth creates a complex environment of multiple data sources, management issues, compliance and security, all within a multi-infrastructure environment.

Our research shows that organisations are facing a 'when, not if' scenario of suffering a cyber security breach and there is a significant disconnect between business expectations and technology reality when it comes to restoring 'business as usual' operations.

Cyber resiliency is a critical consideration for organisations and while a relatively small number of ASEAN organisation in research are mature, the majority are still evolving and enhancing their cyber resiliency operations.

In support of these initiatives, organisations are looking to increase their investment in creating immutable data copies, establishing cleanrooms that are part of integrated data management, backup and resiliency platforms whilst exploring the use of both offensive and defensive AI for cyber security.

COMMVAULT PERSPECTIVE

In today's complex and ever-evolving cyber landscape, organisations must prioritise cyber resilience to ensure the continuity of their business operations and protect their valuable data. The State of Data Readiness Cyber Resiliency Edition report for ASEAN highlights several best practices that can help organisations enhance their cyber resilience capabilities. These best practices include:

Establishing a Proactive Platform-based Cyber Resiliency Strategy across your Enterprise: Organisations should develop a comprehensive and proactive cyber resiliency strategy that focuses on anticipating, withstanding, recovering from, and adapting to adverse conditions, stresses, attacks, or compromises. This strategy should align with the organisation's overall business objectives and incorporate strong incident response plans, backup and recovery systems, and business continuity measures.

Bridging the Gap between Business Expectations and Technology Reality: There is often a disconnect between the time business leaders expect to be back in business after a breach and the time IT professionals require for recovery. Organisations should bridge this gap by setting realistic expectations and investing in technologies and processes that enable faster recovery times. This may include leveraging technologies like data cleanrooms, immutability, and artificial intelligence to enhance data recovery and integrity. The ability to recover at scale is critical and companies must ensure they take a platform approach that integrates all aspects of backup, recovery and resiliency.

Embracing Data Immutability: Data immutability, or the ability to maintain an unchangeable copy of data, is becoming increasingly important for organisations seeking cyber risk insurance. Immutable data provides quicker recovery, better data integrity and compliance, and more effective auditing and forensic capabilities. Organisations should invest in solutions that enable data immutability across multi-infrastructure environments without impacting system performance or increasing data management complexity.

Implementing Data Cleanrooms: Data cleanrooms are controlled environments that allow organisations to securely analyse and manipulate sensitive data without compromising its integrity. These cleanrooms can significantly enhance data recovery post-breach, improve data integrity and confidentiality, and support advanced analytics for forensics. Organisations should leverage data cleanrooms to strengthen their recovery and resiliency stances. Lastly, cleanrooms create an environment where regular testing of incident response and recovery plans can be undertaken cost efficiently and with minimal disruption to business operations.

Leveraging Artificial Intelligence for Cyber Security: Artificial intelligence (AI) can play a crucial role in strengthening cyber security and resiliency. Organisations should adopt AI solutions that can help them detect and respond to cyber threats more effectively. AI can be used defensively for tasks like firewall management and offensively for activities like phishing simulation. By leveraging AI, organisations can enhance their cyber security capabilities and stay one step ahead of cyber attackers.

Engaging Technology Partners: Organisations should collaborate with technology partners to enhance their data management, security, and recovery operations. These partners can bring valuable skills, infrastructure management capabilities, breach recovery expertise, education and training, and governance, risk, and compliance management. Organisations should carefully select partners based on their specific needs and preferences.

By implementing these best practices, organisations can strengthen their cyber resilience capabilities and better protect their data and business operations. It is crucial for organisations to bridge the gap between business expectations and technology reality, embrace technologies like data immutability and cleanrooms, leverage AI for cyber security, and engage with trusted technology partners. These practices will help organisations minimise the impact of cyber attacks, and ensure the continuity of their business operations in the face of evolving cyber threats.

APPENDIX

The research methodology and demographics

Using an online panel approach, TRA conducted an independent quantitative market research survey in December 2023 and January 2024.

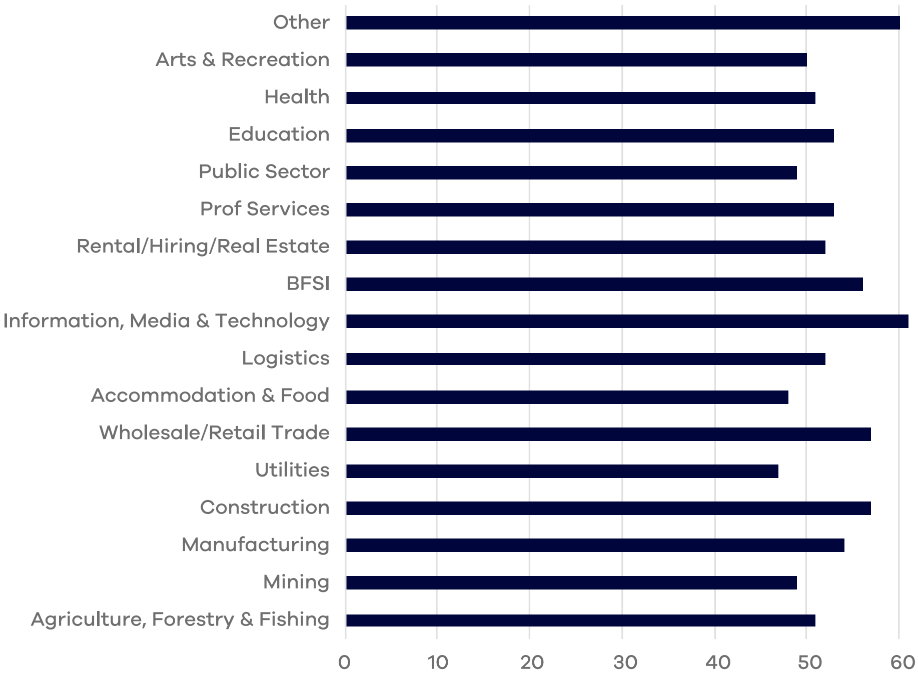
The total sample size is 900 organisations and respondents are CIO/CISCO, IT Leader, IT decision Market and direct reports.

Companies were required to have between 100-199 or 200+ employees and the sample distribution is 50/50 between each group in each country.

Country distribution:

- **Indonesia: 150**
- **Malaysia: 150**
- **Philippines: 150**
- **Singapore: 150**
- **Thailand: 150**
- **Vietnam: 150**

Respondent Company by Industry Sector



ABOUT

Commvault (NASDAQ: CVLT) is the gold standard in cyber resilience, helping more than 100,000 organisations to uncover, take action, and rapidly recover from cyber attacks – keeping data safe and businesses resilient and moving forward. Today, Commvault offers the only cyber resilience platform that combines the best data security and rapid recovery at enterprise scale across any workload, anywhere with advanced AI-driven automation – at the lowest TCO.

ABOUT TECH RESEARCH ASIA (TRA). TRA is a fast-growing IT analyst, research, and consulting firm with an experienced and diverse team in: Sydney | Melbourne | Singapore | Kuala Lumpur | Hong Kong | Tokyo. We advise executive technology buyers and suppliers across Asia Pacific. We are rigorous, fact-based, open, and transparent. And we offer research, consulting, engagement and advisory services. We also conduct our own independent research on the issues, trends, and strategies that are important to executives and other leaders that want to leverage the power of modern technology.

www.techresearch.asia

For further information on acquiring rights to use Tech Research Asia research and content please contact us via our website or directly. Disclaimer: You accept all risks and responsibility for losses, damages, costs and other consequences resulting directly or indirectly from using this research document and any information or material available from it. To the maximum permitted by law, Tech Research Asia excludes all liability to any person arising directly or indirectly from using this research and content and any information or material available from it. This report is provided for information purposes only. It is not a complete analysis of every material fact respecting any technology, company, industry, security or investment. Opinions expressed are subject to change without notice. Statements of fact have been obtained from sources considered reliable but no representation is made by Tech Research Asia or any of its affiliates as to their completeness or accuracy.