# THE STATE OF DATA READINESS

## CONTINUOUS BUSINESS IN FOCUS

ASIA
2nd Edition
February 2025

A Tech Research Asia Insights Report, commissioned by Commvault.

Commvault®

TRA

# INTRODUCTION

## Welcome to the 2nd edition of The State of Data Readiness in Asia

This edition provides insights into the data management, cybersecurity, and regulatory challenges faced by organisations in Asia.

Our first edition in 2024 provided an overview of:

- **Data – it's year on year growth, the infrastructure on which it resided, and the prevalence of dark data;**
- **The top 2 issues impeding data management & security;**
- **Business expectations of the time to recover from a cybersecurity breach and how this differed to the recovery reality; and**
- **An overview of cyber attacks, the use of AI in cybersecurity, data recovery rates and breach awareness.**

For this year, we repeated some areas and expanded our coverage to also include:

- **How changing regulations are impacting organisations' technology strategies;**
- **If companies see a cybersecurity risk when deploying business-focused AI solutions; and**
- **If companies are making progress in strengthening their cybersecurity capabilities – and if so – what is the impact on their ability to maintain operations in the event of an attack or breach.**

Importantly, we were also keen to understand the differences in cybersecurity operations and beliefs between companies that have breached and those that have not.

In that context, we asked if the experience of being breached materially changes a company's view of its operations and capabilities, especially in relation to:

- **The deployment and impact of AI-business tools on a company's cybersecurity risk profile;**
- **Effective incident response and recovery operations; and**
- **Expectations for business recovery in light of a breach.**

We hope that you find value in comparing your organisation to your regional peers and that the report helps you to enhance and strengthen your own data management, recovery, and cyber resiliency capabilities for continuous business.

Sincerely,
Tech Research Asia

**The data provided in this Commvault commissioned TRA Insight Report comes from 1,218 companies in Indonesia, Hong Kong, Korea, Malaysia, Philippines, Singapore, Thailand and Vietnam. Additional information on this sample can be found in the appendix of the report.*

# REPORT HIGHLIGHTS

**Data estates grew year on year, as did the list of regulatory requirements to which organisations must adhere. Enthusiasm for AI continues to be strong even in the face of heightened concerns about the impact on an organisation's cyber and risk capabilities. Interdependent sprawl across infrastructure, workloads and data increases the difficulty of both testing incident response plans as well as maintaining minimum viable business operations in the event of an attack or data breach.**

**The Data Environment:**

- The average growth in data estates in the last 12 months was 40%, an 8% increase over the previous year.
- 63% of companies operate blended data infrastructure environments (multi- or hybrid cloud).
- 38% of organisations lack confidence in understanding all the necessary relationships, metadata, and configurations required to restore business operations if breached.

**The Regulatory Environment:**

- 78% are required to maintain copies of data in different cloud environments to support resiliency capabilities.
- 53% face conflicting regulatory demands for their data across different geographies.
- 52% need to comply with at least four major regulatory acts, 14% are subject to at least six.

**The AI Environment:**

- The integration of AI in business processes complicates compliance with already complex regulations: almost 60% of companies are now subject to AI-related compliance requirements and another 27% will be in the coming year.
- 73% of organisations believe adopting business AI solutions increases the likelihood of a cybersecurity breach, yet this has not prevented deploying AI-business solutions.
- 58% of organisations have not conducted thorough audits on the security implications of AI tools prior to deploying them.
- 46% have comprehensive policies in place to protect AI-generated data.

**The Recovery and Resiliency Environments:**

- 23% rate their ability to operate effectively during a cybersecurity incident as 'excellent'. 12% rate themselves as 'bad' or 'terrible', the rest muddle through.
- 85% have incident response plans (IRPs) in place, however only 30% test all their mission critical workloads as part of IRP activity.
- Of those breached, 83% experienced data exfiltration activity, 50% lost access to all their data, and less than half (41%) recovered 100% of their data.
- 72% of business leaders expect to recover from a cybersecurity incident within 5 days. 23% want to be back in business within 1 day (or less).
- However, 70% of businesses take more than one-week to recover – a significant gap between expectations and reality.
- Of the 68% of companies that had a ransomware demand, 39% paid. Despite 57% of companies having a 'no payment' ransomware policy, when attacked, 34% of those broke policy and paid the ransom.

**Considerations**

- Companies face complicated, sometimes contradictory, regulations. Many Asian governments are expanding their privacy and cybersecurity laws, especially in areas of mandatory breach disclosures, cross-border data transfers and business resiliency.
- Organisations are making progress with strengthening cybersecurity and resiliency capabilities. The impact of AI, the complexity of recovering in multi-infrastructure environments and the disconnect between business expectation and IT reality on responding to attacks and breaches, means effort is still very much a work-in-progress to achieve continuous business.
- Incident response plans are increasingly under a microscope, assessing their efficacy. As the complexity of data environments and regulations increase, organisations must check that the scope, timing and depth of their incident response plans are aligned to maintaining business operations during an attack or breach instead of a reactive, post-incident recovery focus.
- IRPs are important but experiencing a breach is the real test of an organisation's business resiliency.

# BREACH LESSONS

## Does being breached mean better resiliency, improved awareness of issues, and a stronger business resiliency stance?

On balance, yes.

Our data suggests breached companies have a better understanding of their actual capabilities, the complexities of recovery in multi-infrastructure environments, and the reality of what it takes to get back in business including:

- **Clarity on response capability:** 20% more of those breached rated their response to it as *'very unorganised and we scrambled to respond'* compared to those that had not been attacked.
- **More (slightly) realistic resiliency expectations:** Line of business managers in 3-in-10 (29%) of organisations not attacked expect to be 'back in business' within 1 day of a breach. By comparison, of those breached, 11% of those breached expect a 1-day recovery.
- **Comprehensive incident response planning:** 25% more of those breached now test all mission critical workloads as part of their incident response plans compared to those not attacked.
- **Due diligence of AI tools increased post attack:** Companies breached are almost twice as likely to consider internally deployed AI tools as contributing to higher levels of cybersecurity risk (37%) compared to those not breached (19%).
- **Greater AI policy and control oversight:** Those attacked were 26% more likely to implement policies and controls on AI created content and data.

Our data also shows higher cybersecurity maturity levels bring benefits in several operational areas:

- I**mproved data recovery:** Those with low levels of maturity were twice as likely to fail in recovering 100% of their data (39.8% successful) in a breach compared to those with high levels of maturity (80% successful).
- **Lower data lock-out levels:** Low maturity level organisations were 34% more likely to be locked out of data in an attack compared to those with high maturity.
- **Stronger business resiliency:** Companies with high maturity levels were 65% more likely to maintain some level of business operations during an attack compared to those with low levels.
- **Shorter recovery times:** Low maturity companies were 52% more likely to experience a recovery time of 3 months or more compared to companies with high maturity.

Let's dive a little more deeply into some of the insights, starting with the trend in data growth and infrastructure.

# THE DATA ENVIRONMENT

## More of it, more unstructured, fuelled by AI, and subject to more regulations.

Our 2024 data indicated Asian organisations experienced 31% growth in their data in the 12 months to January 2024. 12 months later in January 2025, this growth rate had increased to 40%.

The most cited drivers of increases include:

1. **Maturing digital transformation programmes;**
2. **Adoption of AI solutions including generative AI, large language models and specifically AI-enabled internet of things (IoT) solutions; and**
3. **Increased regulatory compliance requirements.**

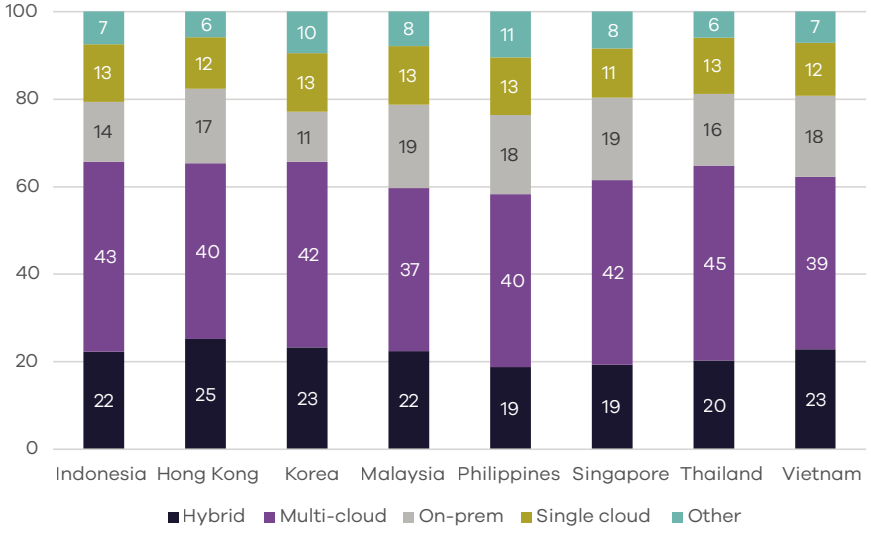
Last year, 60% of that data growth was unstructured. This year it rose to represent 66% of new data created and stored.

Almost two-thirds of organisations (63%) have a multi-infrastructure strategy (multi-cloud or hybrid) for their data estates, 17% are on-premises, and 13% are 'all-in' on a single public cloud environment.

This is similar to last year, and organisations are forecasting minimal changes in the coming 12 months, with only another 6% stating they would *'consider moving to include more cloud in their infrastructure environment in the next year.'*

We dive into some of the key regulations across Asia that have important implications on page 10.

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




# THE REGULATORY ENVIRONMENT

**Changes in data privacy and cybersecurity laws across Asia have significant implications for business technology environments and capabilities. A non-exhaustive list for each country is outlined here.**

**Data Privacy**

| | |
|---|---|
| **Indonesia** | Full implementation of the Personal Data Protection Law (PDPL), including mandatory breach reporting, appointment of Data Privacy Officers, cross-border data controls, non-compliance penalties, and the establishment of a Data Protection Authority. |
| **Hong Kong** | Proposed changes to the Personal Data Privacy Ordinance (PDPO) including mandatory data breach notification, data retention polices, penalties, AI framework models, as well as new cybersecurity law to protect critical infrastructure. |
| **Korea** | Personal Information Protection Act (PIPA) enhancements around consumer trust and compliance with international norms including consent, data breach notifications, chief privacy officer requirements, and overseas data transfers. |
| **Malaysia** | Personal Data Protection Act updated in 2024 including mandatory data protection offices, changes to data breach disclosures, biometric data and cross-border data transfer rules. |
| **Philippines** | Amendments to the Data Privacy Act, digital age of consent, data breach reports for personal information controllers outside of the country. |
| **Singapore** | Multiple changes to the Personal Data Protection Commission (PDPC) guidelines, regulations and fines. |
| **Thailand** | Master plan for the Office of the Personal Data Protection Committee, new cross-border data transfer rules, and compliance requirements. |
| **Vietnam** | Late 2024, Draft Personal Data Protection Law opened for public consultation, encompassing consent, data protection impact assessments, and cross-border data transfers. |

### Cybersecurity

| | |
|---|---|
| **Indonesia** | Along with assessing the Cybersecurity and Resilience Bill, the government also issued regulations around incident reporting, contingency planning and developing incident response teams. |
| **Hong Kong** | Introduction of the Protection of Critical Infrastructure (Computer Systems) Bill including CIO obligations, incident reporting, penalties, risk assessments and security audits. |
| **Korea** | Revisions to the Information and Communication Network Act to include mandatory reporting, compliance inspections, and critical infrastructure resilience. |
| **Malaysia** | Introduction of the Cybersecurity Act 2024 including defined critical infrastructure sectors and mandatory protection requirements, threat management regulatory frameworks, non-compliance penalties, and establishing a National Cybersecurity Committee. |
| **Philippines** | Multiple legislative changes focusing on critical infrastructure industries, workforce development, policy frameworks, and resiliency. |
| **Singapore** | 2024 Amendments to the Cybersecurity Bill including expanded regulatory oversight, critical infrastructure industries, incident reporting obligations, civil penalties, and guidelines for AI security. |
| **Thailand** | Multiple legislative changes including new requirements for critical infrastructure industries, cybersecurity standards for cloud services, and increased governance requirements. |
| **Vietnam** | Proposed Cybersecurity Administrative Sanctions Decree including fines for breaches, non-compliance penalties, as well as the November 2024 Law on Data (into effect in July 2025) regulating data usage, digital data management and data processing. |

So, what does this all mean?

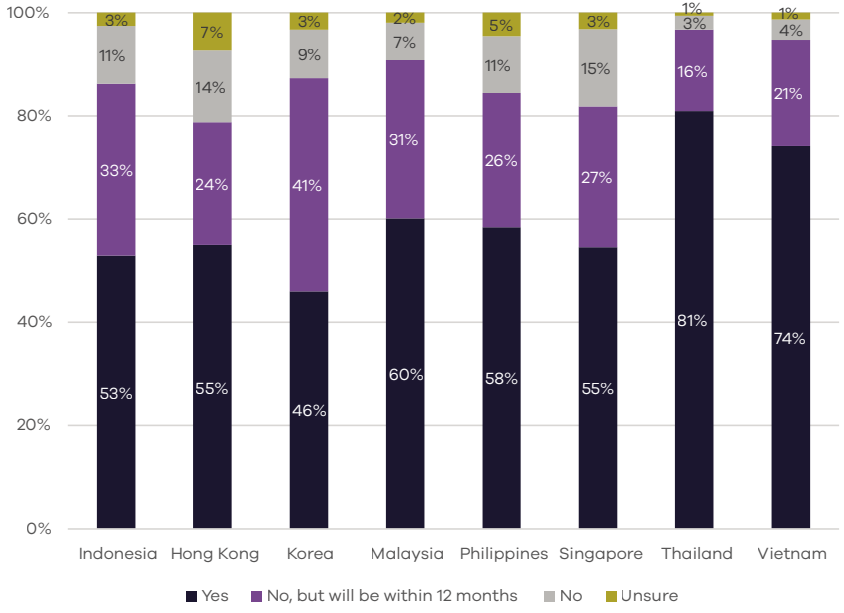
# THE REGULATORY ENVIRONMENT IMPLICATIONS

**Companies face more complexity, increased pressure to strengthen cybersecurity and resiliency capabilities, and AI laws are also coming into effect.**

There's a lot to unbox in the various data privacy and cybersecurity regulations, however three key areas stand out:

1. **Mandatory data breach notifications: Many governments now require (or will do so in the near future) that companies notify authorities of data breaches (in some cases within 24 hours). Along with establishing Data Protection Offices (DPOs), this means data compliance, management and reporting systems will need to be accurate, rapid, and work across multi-infrastructure environments (no easy task).**
2. **Cross-border data transfers: Organisations face multiple, and conflicting, requirements for cross-border data transfers. Data localisation laws also require companies to store certain types of data within sovereign borders.**
3. **Operational resiliency: Regulations are focusing on requiring companies to maintain a minimum level of business operation while subject to data breaches or cybersecurity incidents. Not just about securing data, it involves having continuity plans in place and tested. With multi-infrastructure the most common data environment, companies will need both visibility into their data estates and deep understanding of the dependencies between meta data, applications, configurations and workloads.**

## Is your organisation subject to specific AI regulatory and compliance requirements or legislation




# THE REGULATORY ENVIRONMENT BATTLE

**Already challenging, getting more complicated, and, for some, undermining their ability to respond quickly to cyber attacks or recover rapidly post attack.**

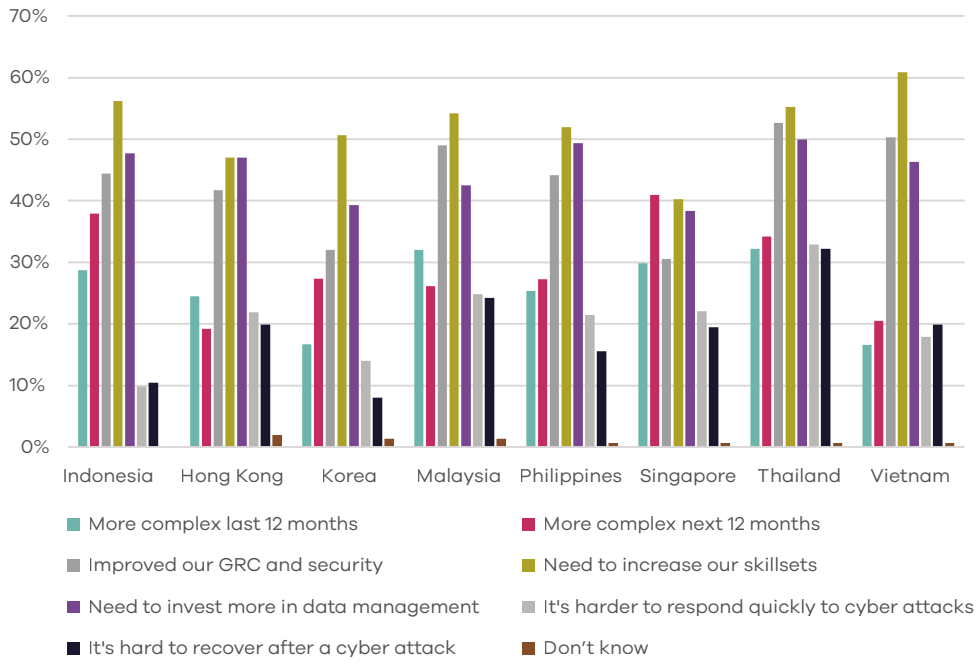
Unfortunately, these challenges are only going to increase:

- 55% of organisations stated that they face, or will face, in the coming 12 months increased complexity and business challenges due to regulatory requirements.
- 52% of organisations noted these laws highlighted a need for additional investment in activities to increase employee GRC and security skillsets.
- 21% reported it's harder to respond quickly to cyber attacks and 19% stated regulations make it hard to recover and restore operations after an attack.
- 53% of organisations state they already experience conflicting regulatory requirements for their data across different geographies.
- 52% of organisations are subject to at least 4 different regulatory and compliance acts (for example, APRA, SOCI, STB, MAS, DORA, GDPR, etc). Another 10% currently 'don't know' what their companies need to be fully regulatory compliant.
- 78% stated regulations now require their business to keep copies of their data in either public or private clouds, distinct from their production data.
- As AI adoption has increased, regulations have moved to incorporate the technology. On average 60% of Asian companies are now subject to AI specific requirements, with another 27% expected to be in the coming 12 months.

Pleasingly, 43% acknowledged that the pain is worth the gain stating that responding to the requirements *'improved our GRC and security capabilities'*.

We've mentioned AI in a number of areas, so it's time to take a slightly closer look on the following page.

Which of the following have impacted your company as regulations have changed in the last 12 months? Please select all that apply, multiple answers allowed.



# THE AI ENVIRONMENT

**The allure of AI outweighs the potential cybersecurity risks and concerns. Deployment rates are high despite concerns that deploying business-focused AI solutions increases the risk of a cybersecurity breach or incident. There's work to be done.**

74% of Asian organisations are currently using business-focused AI solutions.

73% of those using, believe AI contributes to increased risk of cybersecurity breach or incidents:

- **23% believe they bring a 'high risk'**
- **50% believe they bring 'moderate risk'**

With this in mind, and 60% of companies are subject to some form of regulated usage of AI solutions, are companies really undertaking due diligence and assessing the impact AI has on an organisation's risk posture?

Unfortunately, the high levels of AI hype in the market are making this difficult:

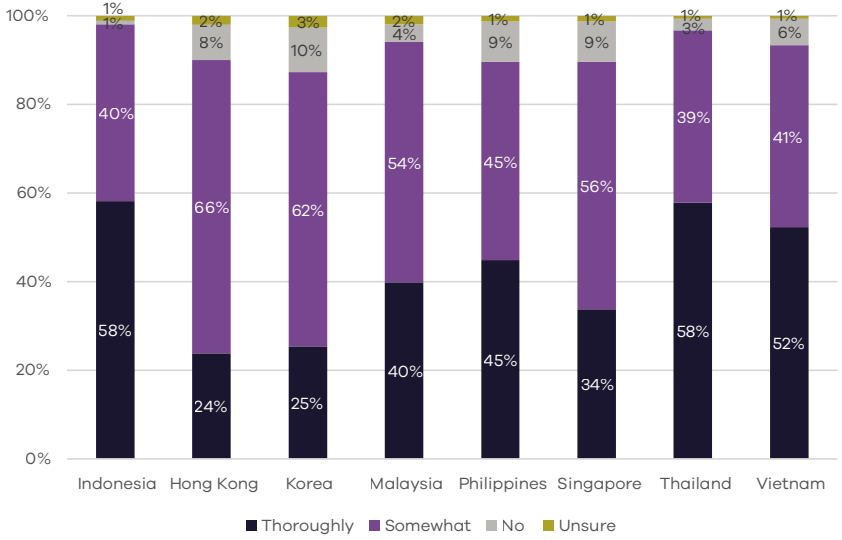
49% of Asian organisations either 'strongly agree' or 'totally agree' with the statement *"The hype around AI makes it difficult to understand the true risk of using AI tools and solutions in our organisation."*

It's understandable. New technology solutions have been oversold on promise since the first 8088 processor PC in the 1970s... still, at least now organisations will be more diligent about vetting solutions before deployment, right?

Well, 42% of them are – our data shows they undertook a thorough audit and review of the security and governance, risk and compliance implications of AI solutions used in their organisation before deployment.

We also see that less than 46% indicate they have comprehensive policies that are part of a broader cybersecurity and data management strategy to protect data and content created by generative AI solutions.

Has your organisation undertaken a thorough audit and review of the security and governance, risk and compliance implications of any of the AI solutions used in your organisation before they were deployed?



# CYBERSECURITY BREACH DATA & IMPACTS

## There continues to be a disconnect between the time business leaders expect to be back in business, and the IT reality.

The 2024 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, still exists in 2025 and is of a similar magnitude.

For business leaders:

- **23% of leaders say an outage of 1 day or less is tolerable.**
- **By the end of day 5, 72% of leaders expect the organisation to have data access restored and be back in business.**

The average time IT leaders reported it took to restore a minimum level of business operation? 3-4 weeks (compared to 4-5 weeks in 2024).

What else did our data tell us?

Close to 100% of organisations experienced some form of cyber attack in the last 12 months and 68% of them were subject to a ransomware demand.

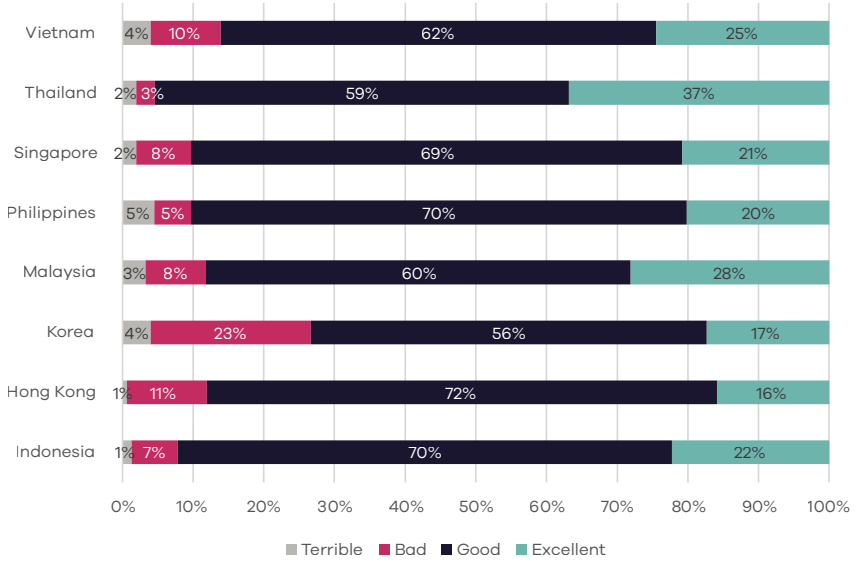
39% paid.

Interestingly, 57% of companies have a 'no payment' ransomware policy and 34% of those still paid, suggesting that reality trumps principles.

Of those attacked:

- **83% experienced data exfiltration;**
- **50% were locked out of their data;**
- **49% lost data. Of these, 41% recovered 100% of data (compared with 35% in 2024);**
- **26% of companies experienced no disruption when attacked; and**
- **24% of companies found out about their breach when contacted by journalists, the attackers, or discovered their data on the dark web.**

How would you rate your company's ability to continue operating during a cybersecurity attack that restricted access to important data?



# THE RECOVERY AND RESILIENCY ENVIRONMENTS

## Testing, testing, testing.

Compared to 12 months ago, companies have made progress strengthening their cyber resiliency:

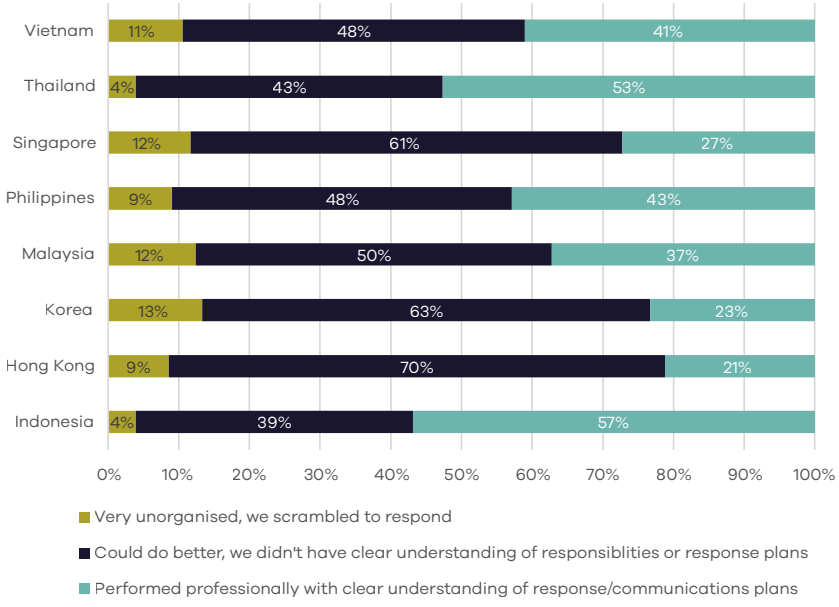
- **85% of organisations have an incident response plan (same as the previous year).**
- **The percentage of companies breached has slightly decreased from 70% (2024) to 68% (2025).**
- **14% score themselves as 'very proactive and mature' when describing their cyber resiliency maturity (an increase from 7% in 2024).**

Interestingly, the data shows the before-and-after attack perspectives.

Prior to an attack, 23% of companies rated their ability to maintain business operations while under attack as 'excellent'.

After an attack, reality sets in, with an average of 53% companies stating they *'could be better, we didn't have clear understanding of responsibilities and response plans', and another 9% declaring '(we were) very unorganised and scrambled to respond'.*

## Which sentence best describes how your company responded to a cyber attack or breach?




# PARTNER ECOSYSTEM SUPPORT

## Identified as a critical support option for 9-in-10 organisations.

When it comes to advice on all things data management, cybersecurity and operational resiliency, the partner ecosystem is trusted by 94% of companies across the region.

More data, more regulations, multi-infrastructure environments and greater demand for continuous business, it's no wonder partners are important.

In this year's report, partners were again identified as bringing a range of advantages and capabilities including:

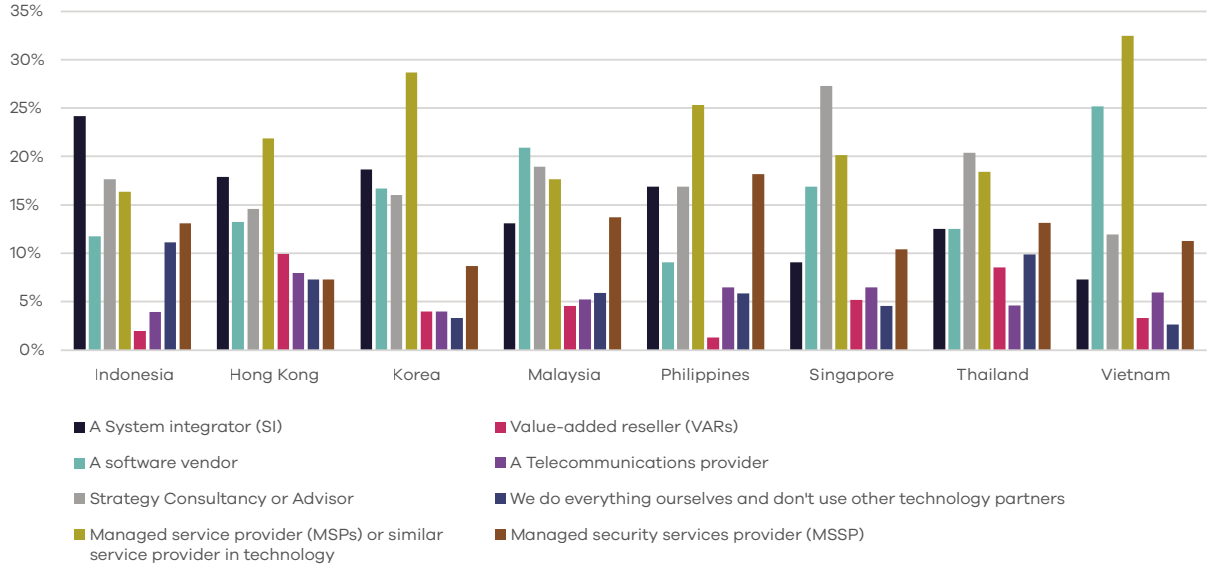
1. **Skills availability;**
2. **Infrastructure, cyber operations (and related vendor) management;**
3. **Breach recovery and incident analysis;**
4. **Education and training; and**
5. **Management of governance, risk, and compliance requirements.**

The most trusted type of partner by country can be seen in the table:

| Indonesia | Hong Kong | Korea | Malaysia | Philippines | Singapore | Thailand | Vietnam |
|---|---|---|---|---|---|---|---|
| SI | MSP | MSP | Vendor | MSP | Strategy consultancy | Strategy consultancy | MSP |
| Strategy consultancy | SI | SI | Strategy consultancy | MSSP | MSP | MSP | Vendor |
| MSP | Strategy consultancy | Vendor | MSP | SI | Vendor | MSSP | Strategy consultancy |
| MSSP | Vendor | Strategy consultancy | MSSP | Strategy consultancy | MSSP | Vendor | MSSP |

*Legend:*
*MSP: Managed Service Provider*
*MSSP: Managed Security Service Provider*
*SI: Systems Integrator*

## Which type of company is your top trusted advisor for data management, cybersecurity and resiliency issues?



# IN CLOSING

Realities differ to plans and theory.

Our data shows that once breached, even the most meticulous plans in some organisations get thrown out the window.

No ransom payment? Sure, we won't pay...yet 1/3 do anyway once the reality sinks in.

Will we be able to maintain business as usual operations if we're breached? Around 90% of companies said 'yes' yet when hit, only 26% managed to maintain operations without disruption when they were attacked.

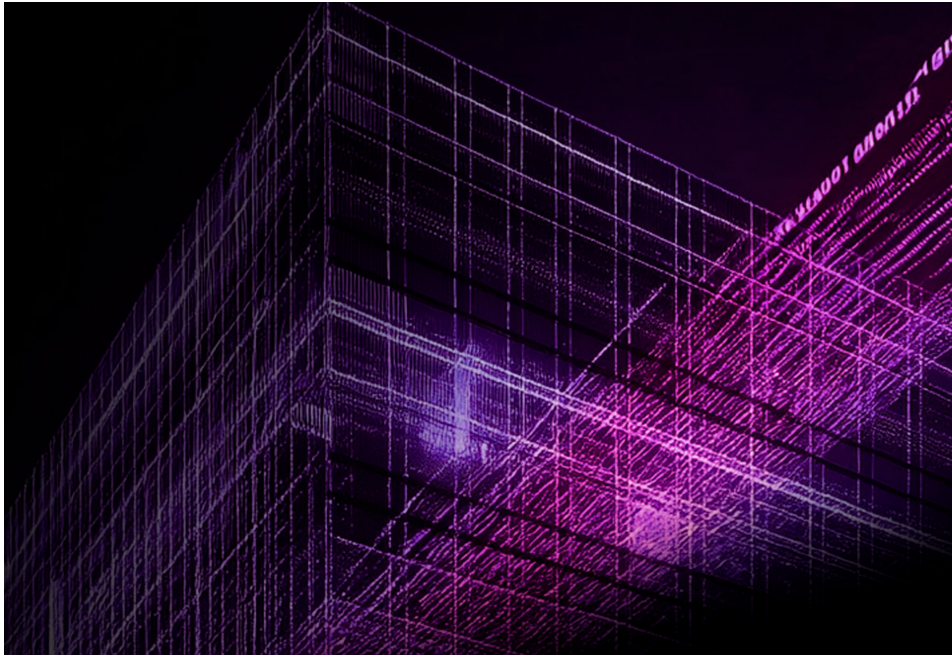
The research also shows that higher cybersecurity maturity levels support improved business resiliency and cybersecurity recovery rates. Strengthening and refining maturity levels requires constant focus and it's not getting easier.

In response to data privacy breaches and cyber attacks, governments have pressed the accelerator on strengthening their regulatory frameworks to support business operations. With this focus on frameworks, GRC, and the ability to maintain business operations during an incident or breach, companies are already under pressure to improve their data management, recovery and business resiliency capabilities.

It is also clear that the integration of AI solutions into business operations presents both opportunities and challenges for data management, cybersecurity and resiliency. There is a need to strengthen governance frameworks, and more thorough testing of IRPs to mitigate these risks. Continuous adaptation of these is also necessary due to the rapid evolution of the AI environment.

As we saw last year, the discrepancy between business expectations for cybersecurity incident recovery times and the IT reality is influenced by a combination of factors including the complexity of IT environments, incident response planning capabilities, resource constraints, operational disruptions, and regulatory compliance pressures.

Addressing these factors through improved planning, smarter incident response strategies, investment in skilled personnel, and enhanced clarity around compliance requirements is essential for organisations to close this discrepancy gap.



# COMMVAULT PERSPECTIVE

In the dynamic and increasingly complex landscape of business operations, continuous business operations is paramount. This report provides a comprehensive overview of the critical factors that organisations should focus on to maintain business continuity, particularly in the face of cyber threats.

**Best Practices for Continuous Business Operations**

1. **Strengthening Cybersecurity Maturity Levels:** The report underscores the importance of enhancing cybersecurity maturity levels. Organisations with higher maturity levels are significantly more resilient during cyber attacks. Specifically, these companies are 65% more likely to maintain some level of business operations during an attack and 34% less likely to be locked out of their data. This highlights the need for continuous investment in cybersecurity measures and the development of robust security frameworks.

2. **Comprehensive Incident Response Plans (IRPs):** Incident response planning is a cornerstone of maintaining business continuity. While 85% of organisations have IRPs in place, only 30% test all their mission-critical workloads. The report emphasises the importance of regular testing and updating of these plans so that they are effective when needed. Companies with high cybersecurity maturity levels are better equipped to handle breaches, with 65% of such companies managing to keep some level of operations running during an attack. This underscores the need for thorough and frequent testing of IRPs to be recovery ready.

3. **Thorough Audits of AI Tools:** The integration of AI solutions can introduce new cybersecurity challenges. The report recommends conducting thorough audits on the security implications of AI tools before deployment. This includes assessing the potential risks and vulnerabilities associated with AI and checking that these tools are securely integrated into the organisation's IT environment. By doing so, organisations can mitigate the risks and maintain business continuity.

4. **Comprehensive Policies for AI-Generated Data:** Protecting AI-generated data is crucial for maintaining business continuity. The report stresses the need for comprehensive policies to protect the security and integrity of data generated by AI systems. These policies should cover data storage, access controls, and data usage to prevent unauthorised access and maintain data availability during and after a cyber attack.

5. **Data Resiliency through Cloud Environments:** Maintaining copies of data in different cloud environments is a key strategy for enhancing data resiliency. This approach means that data can be quickly recovered in the event of a breach or other disruptions. By distributing data across multiple cloud environments, organisations can reduce the risk of data loss and critical operations can continue without significant interruption.

6. **Addressing IT Environment Complexity and Regulatory Compliance:** The complexity of IT environments and the pressures of regulatory compliance can pose significant challenges to business continuity. The report recommends improved planning and investment in skilled personnel to address these challenges. Organisations should develop strategies to manage the complexity of their IT environments and be compliant with relevant regulations. This includes regular audits and assessments to identify and mitigate potential risks.

### The Role of Data Management

Data management plays a critical role in continuous business operations, especially in the context of cyber attacks and breaches. Organisations must have a clear understanding of their data, including metadata, configurations, and dependencies, to effectively respond to and recover from incidents. Higher cybersecurity maturity levels, which include robust data management practices, lead to better data recovery rates, lower data lock-out levels, and stronger business resiliency. The integration of AI solutions, while presenting new challenges, requires thorough audits and comprehensive policies to mitigate cybersecurity risks and maintain business continuity.

### The Impact of Cybersecurity Maturity

This report provides compelling evidence of the impact of cybersecurity maturity on continuous business operations. Companies with high cybersecurity maturity levels are significantly better equipped to handle cyber attacks. These organisations are 65% more likely to maintain some level of business operations during an attack and twice as likely to successfully recover 100% of their data. This highlights the importance of continuous focus and improvement in cybersecurity maturity to support business resiliency.

### The Gap Between Recovery Expectations and Reality

We also continue to observe a significant gap between recovery expectations and the reality faced by companies after a cyber attack. Business leaders often expect a quick recovery, with 72% anticipating a return to normal operations within 5 days. However, the actual recovery time is much longer, with 70% of businesses taking more than a week to recover. This discrepancy can severely impact continuous business operations, though it can be seen that companies with higher cybersecurity maturity levels are better equipped to handle breaches, with these companies being more likely to maintain some level of business operations during an attack.

In conclusion, continuous business operations in the face of cyber threats requires a multi-faceted approach. Organisations must focus on strengthening their cybersecurity maturity levels, implementing and regularly testing comprehensive incident response plans, conducting thorough audits of AI tools, and maintaining robust data management practices.

By addressing the complexity of IT environments and regulatory compliance pressures through improved planning and investment in skillsets, organisations can significantly enhance their ability to maintain business continuity and recover from cyber attacks effectively.

# APPENDIX

## The research methodology and demographics

Using an online panel, TRA conducted an independent quantitative market research survey in December 2024 and January 2025.

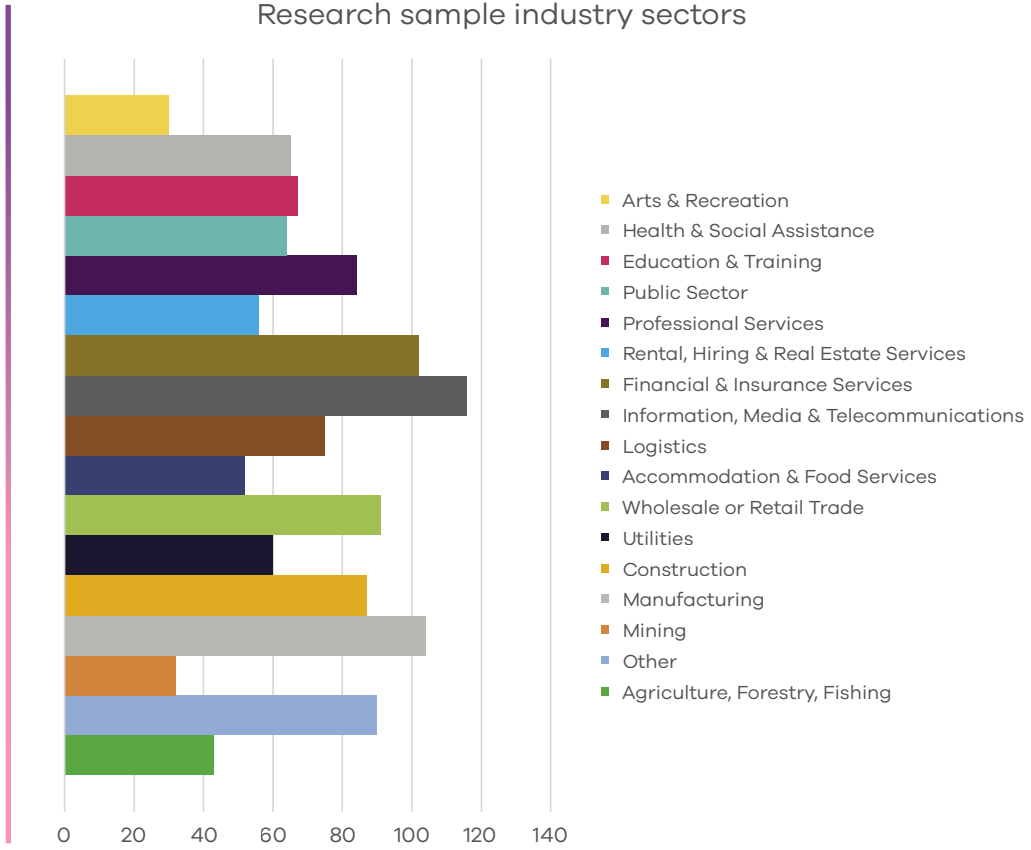
The total sample size is 1,218 organisations and respondents are CIO/CISO, IT Leader, IT decision maker and direct reports.

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: 153**
- **Hong Kong: 151**
- **Korea: 150**
- **Malaysia: 153**
- **Philippines: 154**
- **Singapore: 154**
- **Thailand: 152**
- **Vietnam: 151**

## Research sample industry sectors




# ABOUT

Commvault (NASDAQ: CVLT) is the gold standard in cyber resilience, helping more than 100,000 organizations 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



Commvault®

TRA