Commvault

The State of Data Resilience

ASIA
3rd Edition
April 2026

A Tech Research Asia Insights Report (now part of Omdia), commissioned by Commvault

Omdia
by informa techtarget

Introduction

The 3rd edition of this report series focuses on how organisations across Asia are approaching the issues of cyber resiliency and what impact artificial intelligence is having in this context.

From the last 2 editions, we have continued our focus on data that readers identified as important (including trends in data infrastructure, the gap between business expectations of breach recovery and the technological reality) alongside research and analysis into the following areas:

- **The significant issues impacting cyber resiliency strategies in an era of both regulatory change and growth in artificial intelligence (AI).**
- **How organisations perceive the impact of AI solutions on trust, transparency, and resiliency, as well as the key requirements needed from AI tools to support cyber resiliency needs.**
- **The differences in adoption of identity management strategies for human and non-human (e.g. Agentic AI), how these impact cyber resiliency, and the common hurdles organisations face.**
- **The disconnect between business expectations on time to recover after a breach and the actual time needed, and why this places pressure on paying ransomware demands from threat actors.**
- **Lastly, we look at paying a ransom versus building resiliency and why following a minimum viable company (MVC) approach when under attack is more effective than paying a ransom demand.**

We finish our report with an overview of how companies see partner skills evolving as organisations move from a recovery to resiliency operational capability.

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

If you're curious about the experience of organisations in Australia and New Zealand (ANZ) look for our sister report **The State of Data Resilience, ANZ, 6th edition, 2026.**

If You Only Read One Page, Read This

Organisations are shifting from a defend-and-block cybersecurity posture to a get-hit-and-keep-going cyber resilience mindset. As regulations gradually propel organisations towards a minimum viable company (MVC) model, the weaponisation of AI by threat actors increasingly makes a breach feel inevitable.

AI, particularly agentic AI, is emerging as both a blessing and a curse. Data indicates that AI adoption intent and allocated AI budgets are set to rise throughout 2026, with agentic AI tools permeating cybersecurity, IT, and broader business operations. Yet many organisations still fail to perform appropriate due diligence on the risks these tools introduce before deploying them, and companies say they cannot fully trust whether the tools are compromised, underperforming, or breaching governance and compliance obligations.

A gap remains between the time frames that line-of-business executives expect to be back up and running and the actual recovery realities. Over time, the data suggests that expectations for a rapid return to a minimal operating level have risen, whilst tolerance for prolonged outages (beyond 5 days) has declined.

These heightened recovery expectations add further pressure on organisations in the midst of a breach. The imperative to 'keep the lights on', combined with the complexity of many recovery environments, makes it almost inevitable that some organisations will opt to pay the ransom, hoping to quickly resume operations. This is a high-risk tactic that often backfires when the threat actor either withholds the data or restores it only to strike again, demanding yet another ransom.

As organisations move from defend-and-block to resiliency, the skills they expect technology partners to bring to support resiliency operations also change. They expand into more extensive requirements that include, alongside data:

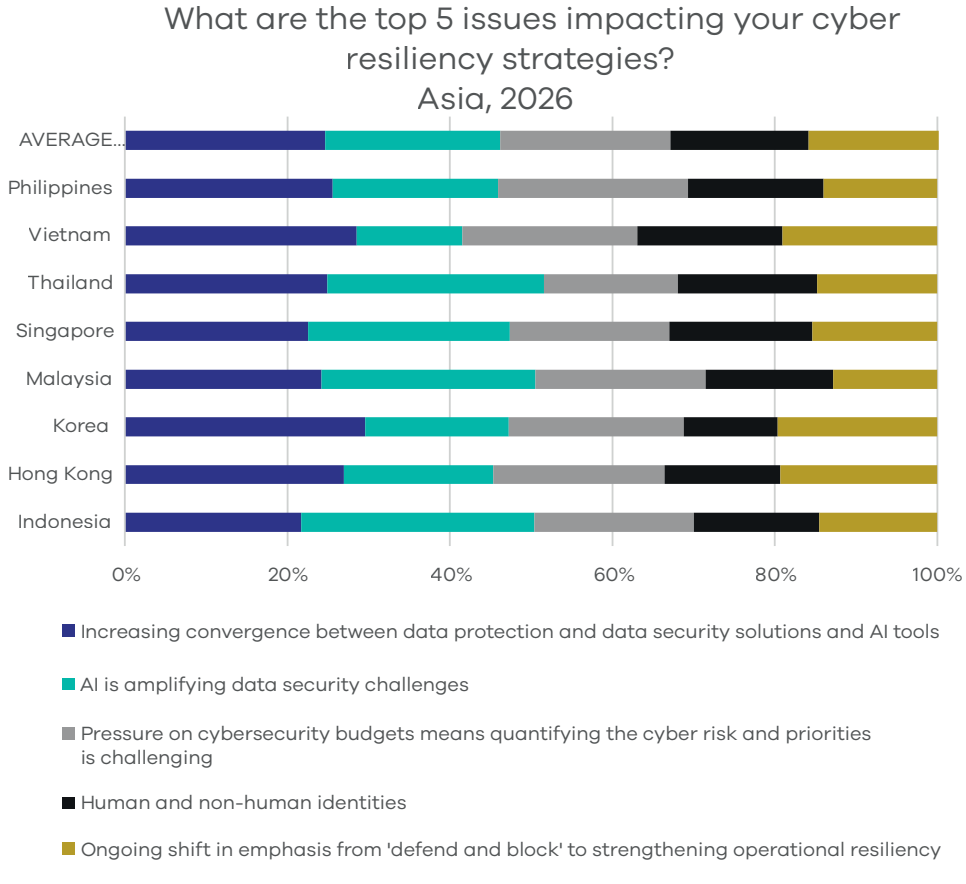
- **Backup capabilities and infrastructure management;**
- **Expertise in cyber resiliency (e.g. digital forensics and breach investigation);**
- **AI solutions (integration, regulatory and compliance); and**
- **Identity access and management (advanced automation provision/deprovision and access controls, AI orchestration and human/non-human workflow integration).**

Top 5 factors impacting cyber resiliency

Across Asia, cyber resiliency is establishing itself as a board and executive-level priority for organisations. Shifts in cybersecurity strategy, addressing AI and budget considerations are critical influences.

Driven by year-on-year growth in data estates, expanding regulatory requirements, and sustained high levels of ransomware activity, our research reveals the top 5 most important cyber resiliency issues companies are grappling with:

1. Increasing convergence between data protection and security tools and AI tools means organisations can benefit as reactive, manual processes move towards an automated, predictive, and intelligent state… if they're ready for it.
2. The amplification of data security challenges by artificial intelligence (AI) amongst other problems including the speed and scale of attacks, adaptive malware, and exploiting business AI environments.
3. Cybersecurity budget considerations means quantifying cyber risk and priorities is even more critical, however the speed of change and deployment of AI solutions sometimes compromises due diligence prior to deployment.
4. As agentic AI solutions become more common risk, identity management environments will need to evolve to more effectively address non-human data access, security, and governance requirements.
5. The shift from defend-and-block to establishing a minimum viable company is triggering a change in established cybersecurity operations.


What are the top 5 issues impacting your cyber resiliency strategies?
Asia, 2026
AVERAGE...
Philippines
Vietnam
Thailand
Singapore
Malaysia
Korea
Hong Kong
Indonesia
0%
20%
40%
60%
80%
100%
Increasing convergence between data protection and data security solutions and AI tools
AI is amplifying data security challenges
Pressure on cybersecurity budgets means quantifying the cyber risk and priorities is challenging
Human and non-human identities
Ongoing shift in emphasis from 'defend and block' to strengthening operational resiliency

Data infrastructure & growth

Data growth rates have re-accelerated. As with previous years, multi-infrastructure environments are the default location.

The average yearly growth in data estates across Asia continues to be above 30% for three years we have undertaken this research.

These sustained increases reflect a combination of factors, including AI-driven data generation, richer telemetry, expanding regulatory retention mandates, and ongoing digital transformation initiatives.

This growth is re-introducing upward pressure on storage, protection, compliance complexity, and costs, especially where dark data is prevalent and data lifecycle management remains immature. Mishandled agentic AI can further intensify these challenges (as explored later in this report).

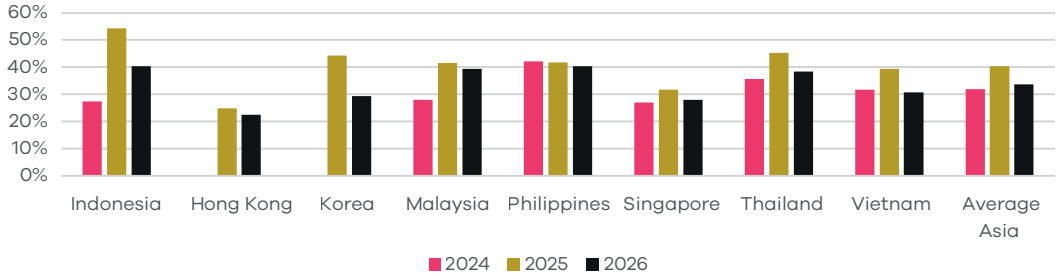
As our previous research has shown, a multi-infrastructure (i.e. hybrid and multi-cloud) environment for data and workloads currently continues to be the favoured approach for the majority of organisations.

Amongst our cohort, Indonesia, Korea and Singapore show the highest levels of multi-infrastructure usage whilst Philippines and Hong Kong are lowest. It should be noted however that even those two countries show multi-infrastructure usage at 59% and 62% of companies respectively.

From recovery and cyber resiliency perspectives, our research revealed several multi-infrastructure common obstacles for organisations to overcome.

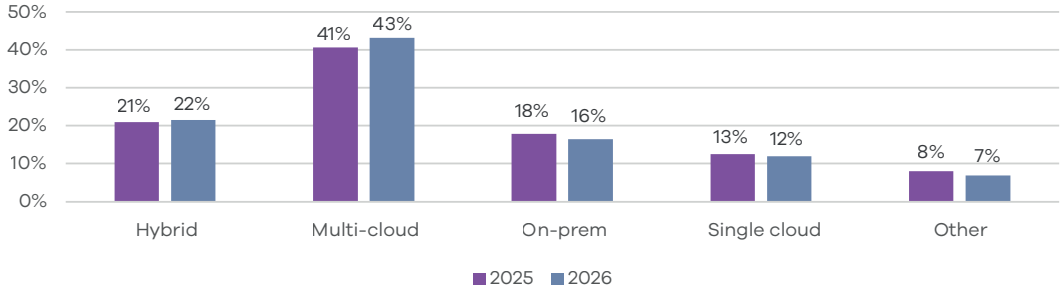
By how much did your data estate grow (or shrink) in the last 12 months?

2024-2026



Which best describes your infrastructure approach for your data and workloads?

Asia, 2025-2026



Top 5 multi-infrastructure issues undermining resiliency

A multi-infrastructure data strategy brings benefits, as long as common obstacles are recognised and addressed.

The multi-infrastructure approach reflects a 'best-fit' location for workloads, localisation requirements, and requirements for data to reside in different clouds (in some instances).

As data estates grow through more unstructured data and AI generated content, the fragmentation of tools and skill sets across both cloud and physical infrastructure alongside this also increases the difficulty organisations will experience in maintaining consistent security controls, visibility, and recovery capabilities.

We asked organisations to identify the most significant obstacles faced in across cybersecurity, resiliency, and data management operations. The top 5 are listed on the following page.

Cybersecurity	Cyber Resiliency	Data Management
Cross cloud solution incident response teams have disparate skills sets **(53%)**	Reduced efficiency resulting from poor storage and data lifecycle management **(49%)**	Our ability to recover after an attack or breach is too slow **(42%)**
Our threat detection performance is not quick enough **(40%)**	Difficulty confirming integrity and cleanliness of backups **(41%)**	Lack of current recovery playbooks adaptable for hybrid attacks **(35%)**
Our ability to recover after an attack or breach is too slow **(38%)**	Incomplete or out-of-date inventory of data and critical systems **(40%)**	Difficulty confirming integrity and cleanliness of backups **(32%)**
Difficulty confirming integrity and cleanliness of backups **(36%)**	Disparate tools or processes across different environments **(39%)**	Our threat detection performance is not quick enough **(31%)**
Lack of current recovery playbooks adaptable for hybrid attacks **(34%)**	Our ability to recover after an attack or breach is too slow **(38%)**	Disparate tools or processes across different environments **(31%)**

AI spending intent and agentic AI adoption

AI intent is clear, budgets are increasing, and companies are making progress around policies to protect AI generated content

As noted earlier, AI is both fueling data growth and being positioned as a key enabler of resiliency and cybersecurity initiatives. More data created means more complex data infrastructures to manage and more investment required. AI spending is set to rise through 2026, with 95% of organisations increasing their budgets, and 36% lifting spend by more than 25% compared with 2025.*

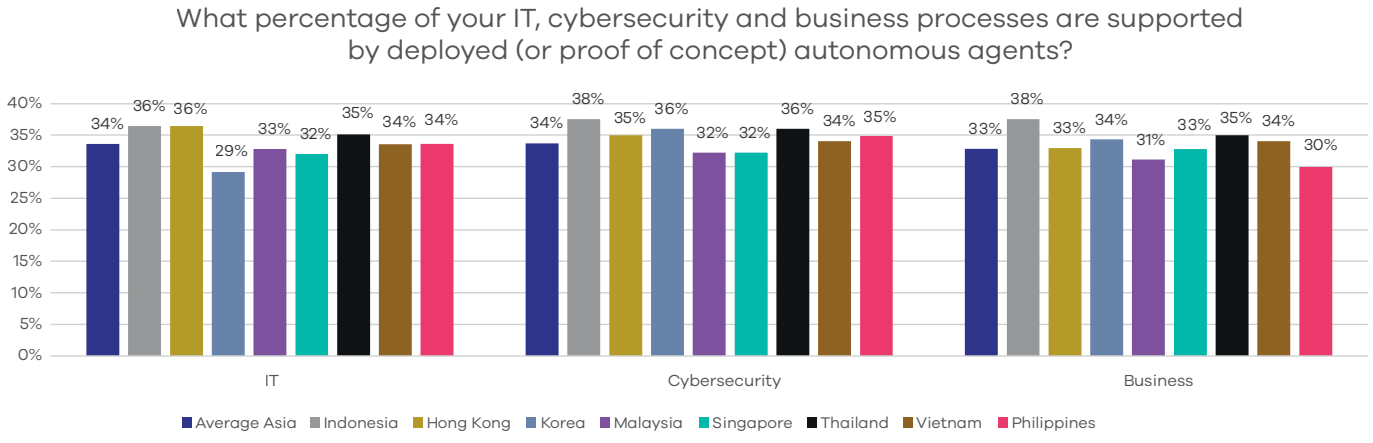
Agentic AI (autonomous agents) are capturing a substantial portion of overall AI budgets. The data indicates that agentic AI is now embedded across multiple facets of business operations, spanning IT, cybersecurity, and core business processes.

On average in Asia, more than 33% of organisations are trialling or deploying agentic AI across these three domains.

As data estates expand and AI adoption accelerates, it is critical that AI-generated artefacts are governed with the same rigour applied to traditional data assets. Encouragingly, there has been clear progress: in 2026, 66% of organisations report having governance, risk and compliance (GRC) policies to safeguard AI-generated data and content, up sharply from 29% in 2025.

However, our data also reveals 2 critical issues influencing the success of organisations' resiliency capabilities.

Source: Omdia AI Market Maturity September 2025


What percentage of your IT, cybersecurity and business processes are supported by deployed (or proof of concept) autonomous agents?
40%
35%
30%
25%
20%
15%
10%
5%
0%
34% 36% 36% 29% 33% 32% 35% 34% 34%
34% 38% 35% 36% 32% 32% 36% 34% 35%
33% 38% 33% 34% 31% 33% 35% 34% 30%
IT
Cybersecurity
Business
Average Asia
Indonesia
Hong Kong
Korea
Malaysia
Singapore
Thailand
Vietnam
Philippines

Organisations lack trust in their AI tools

If deploying AI early and quickly for competitive advantage, make sure you don't overlook due diligence.

The 2 flaws we mentioned on the previous page? **Speed to deploy** and **a lack of trust and transparency** in AI processes.

Some organisations are rushing AI tools into deployment without necessary due diligence.

In our 2025 report we noted that "Currently, the allure of AI benefits outweigh the potential cybersecurity risks and concerns."

This year, when asked whether they had undertaken a thorough audit and review of the security and GRC implications of AI solutions before deployment, only 42% of Asian organisations indicated they had conducted a 'thorough' assessment.

There is clearly a desire to move quickly to gain maximum competitive advantage through deploying AI.

However, even when deployed, on average only 43% companies in Asia are 'very confident' they are getting the right outcomes from their AI tools. This lack of trust is multi factor too, spanning mistakes, compromised tools, GRC breaches, and data guardrails.

With this in mind, let's take a deeper look into cybersecurity, resiliency, and the use of AI.

"How confident are you that your business can identify the following AI errors?"

Made a mistake	**41%**
Been compromised	**43%**
Broken compliance/governance requirements	**44%**
Compromised data access guardrails	**46%**

Cybersecurity, resiliency and the use of AI

There is no question AI is changing the cybersecurity landscape as well as how organisations build resiliency capabilities.

Despite the concerns highlighted on the previous page, the research shows that fewer than 10% of Asia Pacific organisations have no plans to use AI*.

If anything, the data underscores AI's rapid transition from an experimental capability to a core element of contemporary security strategies and architectures.

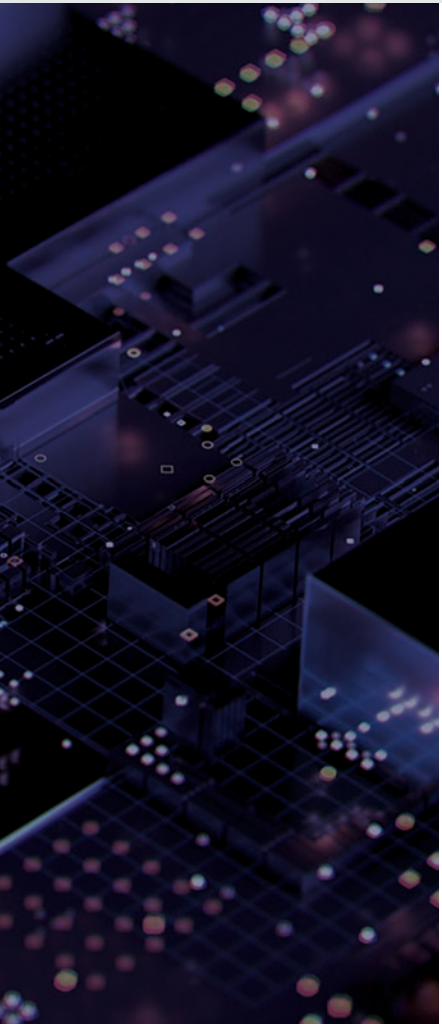
For those adopting and deploying AI, the motivations are clear: increase productivity, lower costs, accelerate and scale automation, and reduce risk and cybersecurity exposure.

So, what are the 3 most common use cases for AI-augmented cybersecurity solutions?

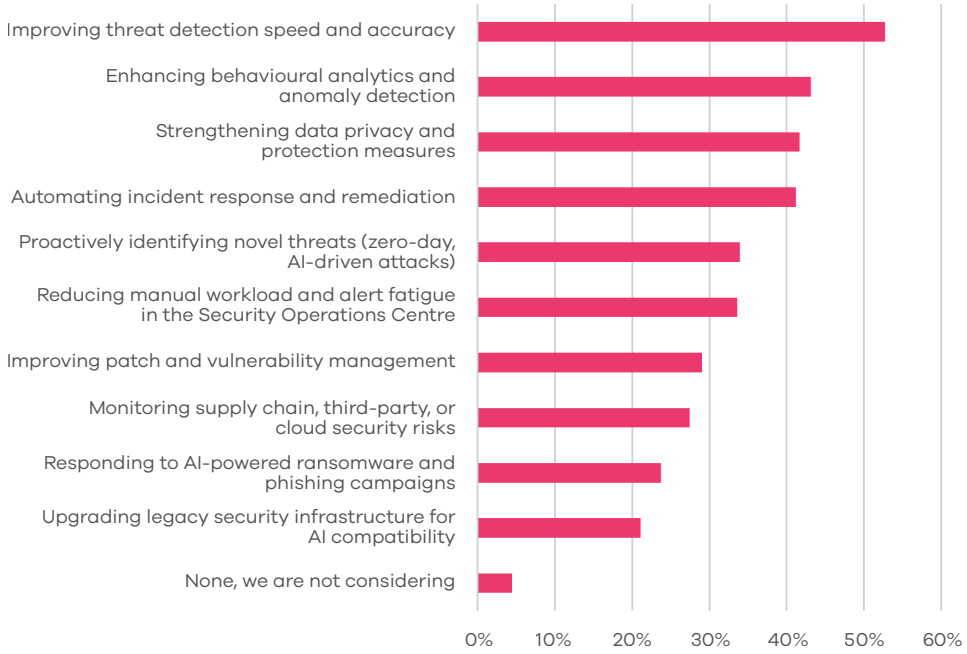
1. Quicker detect and threat response and improved accuracy, critical in Asia where companies face skills shortages as well as increasingly AI-augmented cyber attacks.
2. Enhanced analytics and anomaly detection, especially across hybrid environments.
3. Boosting data privacy controls at scale across multiple jurisdictions and supporting compliance with the growing focus amongst Asia on privacy regimes as well as strengthening cyber resiliency.

With organisations clearly focusing on improving their resiliency capabilities through AI, what are the main solution attributes they're looking for from vendors?

Source: Omdia AI Market Maturity September 2025



What are the most important cybersecurity issues you want to address with AI-augmented cybersecurity tools?
Asia, 2026



AI for Cyber: Solution requirements

Move fast, but don't break things. Speed, trust, and compliance are the top considerations for companies looking to boost their resiliency capabilities with AI tools.

Echoing the trust concerns outlined earlier in this report, the most prized attributes are explainability and auditability. These capabilities enable security, risk and compliance teams to understand, justify, and review AI-driven decisions and actions.

Seamless integration into existing tools and workflows, rapid and accurate threat detection, and strong automation and orchestration of incident response are all essential for AI to effectively augment security and resiliency operations.

For Asian organisations the key requirements are:

1. The ability to explain model decisions (increasingly so as legislation will begin to require this where it relates to PII data, individual's rights and interests) and to consider their transparency.
2. Integration with existing security tools and workflows to boost the existing capabilities, improve response times and minimise management complexity.
3. Improving the accuracy and speed of threat detection by continuously analysing data sets, telemetry and other signals in real-time and correlating signals with patterns to identify threats faster.

One issue that our research surfaced concerns the implications for agentic AI on organisations' identity management capabilities and we delve more into this in the coming commentary.

What are the key AI cyber solution requirements to support resiliency?
Asia, 2026

Human and non-human agents

There is a clear lag with organisations' cyber resiliency planning and capabilities incorporating non-human agents.

73% Asian firms incorporate managing human identities in their cyber resiliency plans. Whilst not perfect, it indicates the relatively maturity and understanding of human identity management across business and technology operations.

However, by comparison, the inclusion of non-human agents is much lower, currently standing at 34%.

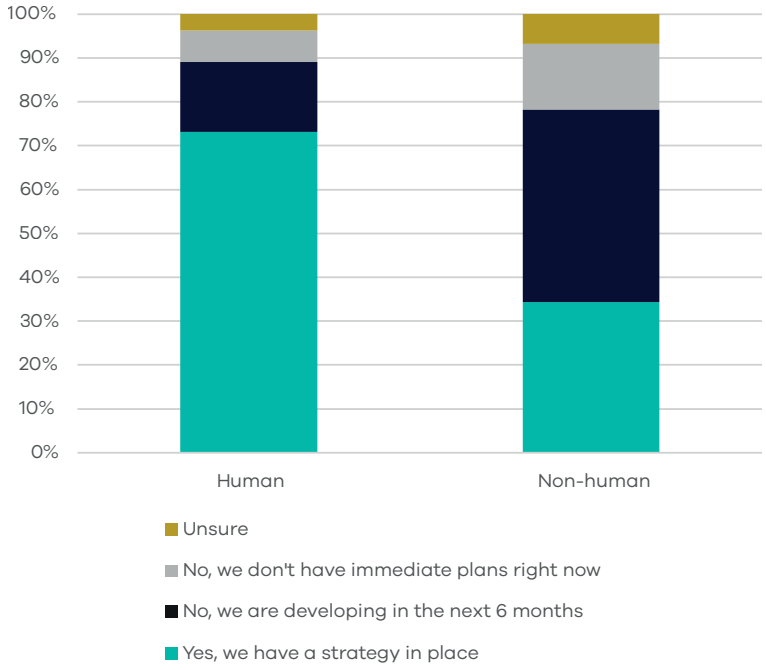
Even for those organisations currently not using their own agentic AI, some of their suppliers and customers will be, and building agent policies and strategies into cyber resiliency plans is critical.

A number factors explain this lag, including:

- Cyber resiliency frameworks have historically focused on human risk, with established playbooks for phishing, insider threats, training, role-based access, etc. tied to people. Equivalent standardised approaches for AI agents are less mature.
- Human users are visible, regulated, and auditable, making them a central focus for governance, compliance, and board reporting. By comparison, non-human agentic AI identities are often poorly inventoried, loosely owned, and sometimes treated as shadow IT.
- Budget, skills, and processes in cyber resilience are still oriented toward awareness programs, behavioural change, and human control, leaving fewer dedicated resources and metrics to design, test, and rehearse specific to autonomous AI agents.
- Agentic AI introduces fast-evolving, potentially poorly understood risks (ephemeral identities, over-permissioned agents, prompt injection, agent-to-agent escalation), and many organisations are still in experimentation mode.

For those considering using agentic AI, our research revealed several key challenges to consider on the following page.

Does your cyber resiliency plan incorporate managing identities for both human and non-human (e.g. Agentic AI solutions engaging with other agents) identities?
Asia, 2026



Agentic AI and identity management challenges

Agentic AI. A blessing and a curse.

As noted earlier, organisations in Asia are piloting and deploying agentic AI across multiple domains, including cybersecurity, IT, and broader business operations.

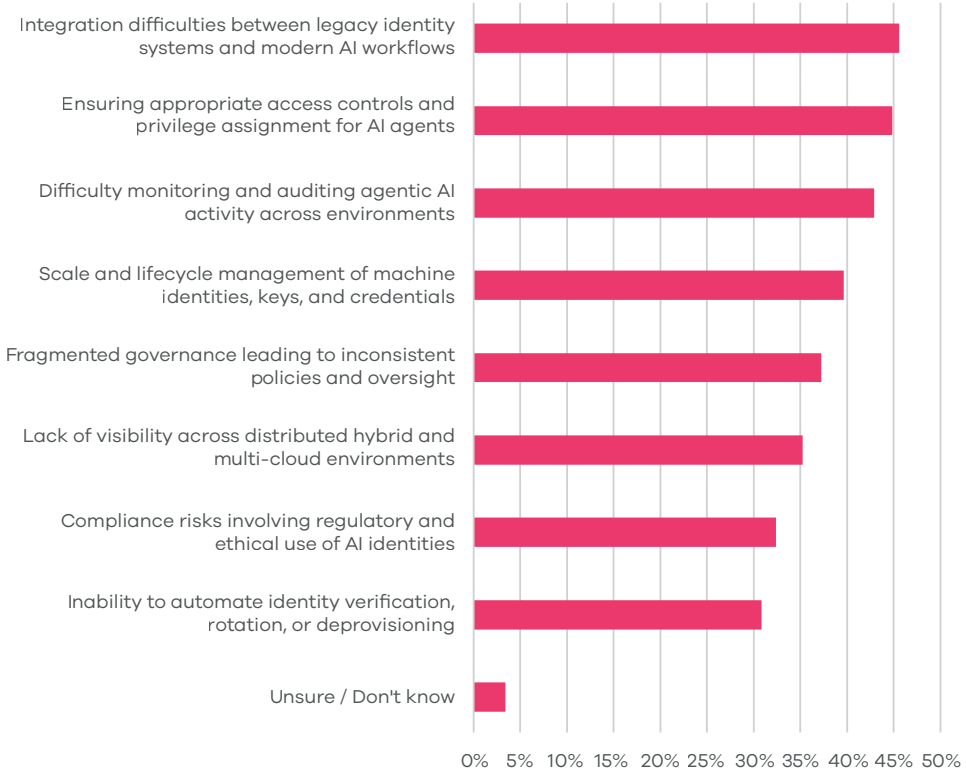
These agents interact with many parts of the business including customers, partners, suppliers, and employees, and in doing so can elevate an organisation's risk profile across customer trust, cybersecurity, and recovery, among other areas.

Our data indicates that organisations recognise the extra complexity agents introduce with 78% of Asian companies reporting that agentic AI has a medium or high impact on complicating both identity management and resiliency operations.

What are these complications?

- Difficulties integrating legacy, human-centric identity management systems with those supporting AI workflows, as the scale and interconnection of machine identities can strain capabilities and agent life-cycle management.
- Managing access and privileges for non-human agents, given the dynamic and ephemeral nature of agents being spun up and down, places greater demands on existing controls.
- Difficult with monitoring and auditing agentic AI activity across environments which is exacerbated by companies having low levels of confidence and trust that AI tools are performing as intended.

Top challenges for identity management with companies using agentic AI. Asia, 2026



Breach recovery expectations and reality

Business executives want to be back in business within 5 days. The reality is somewhat different.

Since the inception of this research in Asia we have tracked the disconnect between the time business executives expect to be operational after a breach or other cyber incident and the time actually required to be back in business from a technology reality.

For the third year, this disconnect still exists. Companies have more data, more locations, more workloads, more regulations, and more complexity.

For Asian business leaders, quickly resuming business operations is the critical factor. On average 29% expect to be operational within 1 day post incident. After 5 days, that number increases to 81%.

The reality?

On average, time to recover to a minimal level of operation is 28 days for Asian companies.

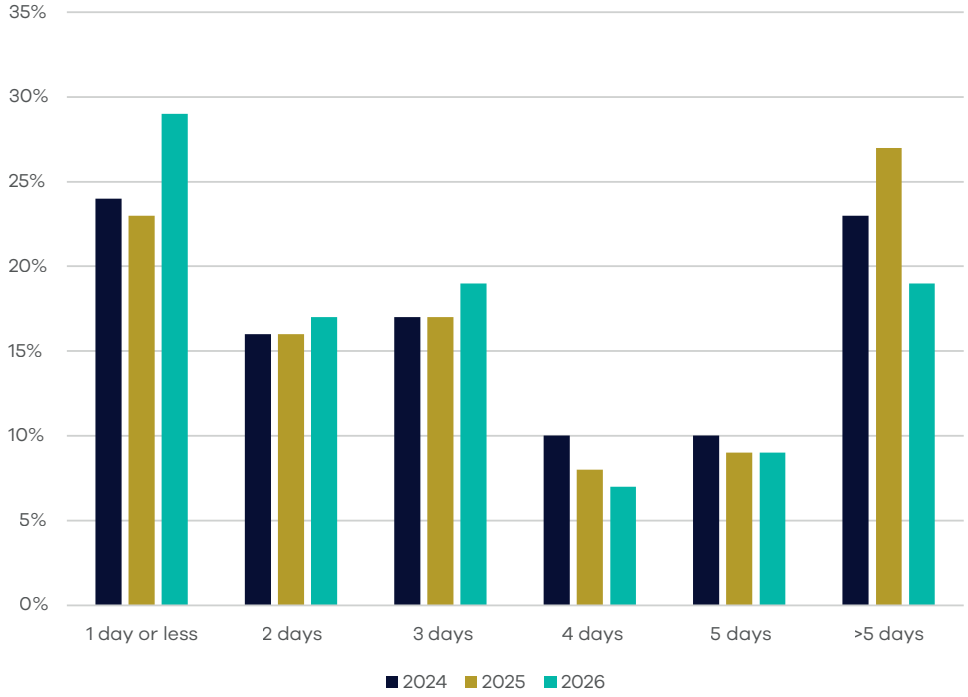
Whilst addressing the breach incident, only 23% of organisations stated they were able to maintain operations without any impact, 66% could operate in a 'limited state' and 11% were unable to function.

The silver lining? Despite increased complexities, on average, the time to recover to a minimal operational level has fallen from 42 days in 2023 to 28 days in 2026.

If breaches are ultimately inevitable, how can you avoid disruption to your business, customers, suppliers, and employees in the shortest time available?

It's understandably why some companies simply want to pay the ransom and 'move on'.

For how long could your business tolerate an outage due to a cybersecurity incident?
Asia, 2024-2026



Ransomware payment effectiveness

Pay the ransom? Sure, roll the dice and hope criminals are feeling 'generous'.

To pay or not to pay?

In contrast to the ANZ data, Asian organisations are more willing to pay ransom demands, however for those that do, there is no guarantee that data access will be restored.

Amount of companies that have been targeted
An average of 44% of companies in Asia surveyed report being targeted with ransomware in the last 12 months.

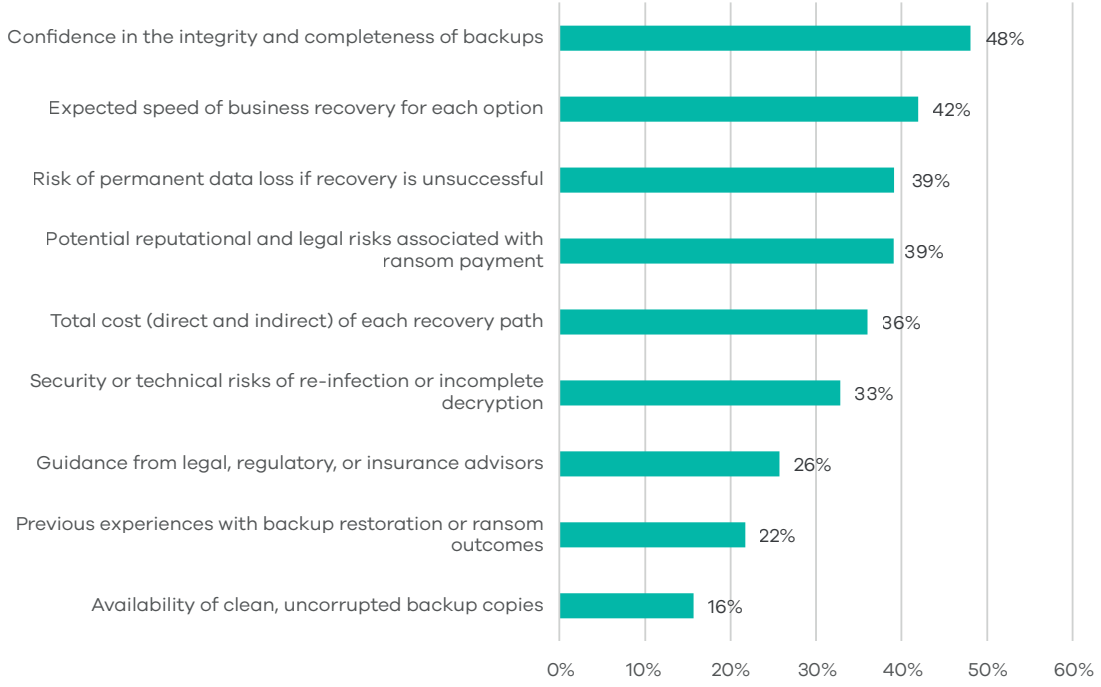
Which factors do they consider when deciding to pay?
Considerations range from the speed of recovery, to cost and risk implications. The factors influencing Asian organisations are revealed in the table to the right.

Do they pay?
Whilst the policy may be to not pay, once breached some companies do buckle under operational and time pressures.

On average 40% of Asian organisations stated they paid the demand, with companies in Malaysia (60%), Indonesia (60%) and Thailand (55%) being more willing.

Does it work?
Of those that paid ransoms, 31% stated it didn't work as the threat actor did not release the data, or if they did, quickly attacked again, demanding additional payment.

When deciding whether to pay a ransom or attempt to restore from backups after a ransomware attack, which factors most influence your organisation's decision?
(Multiple answers allowed)



Defining your Minimum Viable Company (MVC)

Having a defined MVC strategy for both business and technology operations significantly boosts the chance of keeping the lights on when attacked.

Broadly speaking, minimal viable company (MVC) planning needs to incorporate technology, cultural, and business considerations starting with the question of 'what is the bare minimum my business requires to continue to operate and serve customers?'.

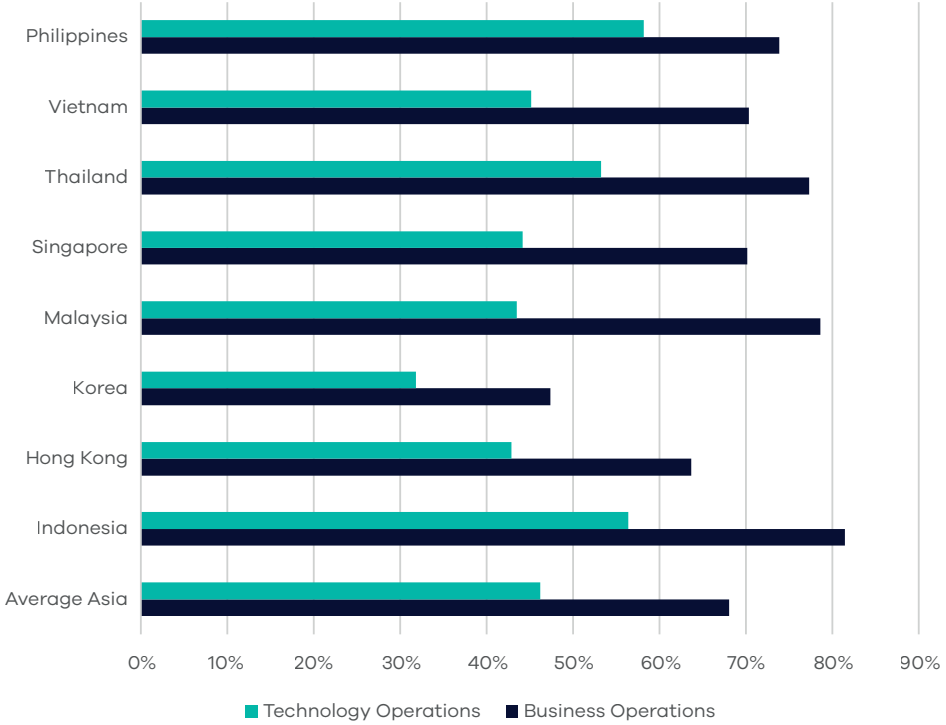
Our data shows that clearly identifying minimum technology requirements (to provide a base level of business operations during an attack) significantly improves the chance of recovery.

Asian organisations with defined minimum levels of operational business requirements linked to clear technology capabilities are 3.2 and 1.6 times respectively more likely to maintain operations when attacked and recover faster, than those with an undefined level.

- 68% of Asian organisations have defined MVC requirements for their business operations.
- By comparison, 46% have defined MVC requirements for their technology environments.

There is much to consider and unsurprisingly, many organisations look to technology partners to help build and support cyber resiliency capabilities. As companies move from traditional backup and recovery operations to cyber resiliency, partner skills and competencies also change, as we outline on the following page.

Have you defined a MVC capability for your business and technology operations? 'Yes', Asia, 2026



Partner skills matrix

Early in our report we noted the move from defend-and-block to establishing a minimum viable company capacity.

For many organisations, they are now looking to partners that can offer a holistic skill set spanning multiple areas including data infrastructure management, cyber resiliency capabilities, AI skills and knowledge, and proficiency in identity management across both human and non-human agents.

Here are the top skills that companies need from their partners across each of these areas.

Data Infrastructure	Cyber Resiliency	Artificial Intelligence	Identity Access Management
Deep, technical proficiency in modern cloud, network and platform management	Backup and data protection management	Expertise with all types of data formats, structured, unstructured, semi-structured, media (video, audio) and collaborative (e.g. emails).	Real-time monitoring and detection of suspicious identity activity
Advanced cybersecurity expertise for threat prevention and compliance	Ransomware remediation and negotiation support	Advanced AI model development and seamless integration with organisational systems	Strong governance, compliance and privacy frameworks
Proactive monitoring, incident detection and rapid problem resolution	Digital forensics and breach investigation	Data management, access, regulatory and compliance skills	Advanced automation for provisioning, deprovisioning and access control
Ability to integrate, automate and optimise diverse legacy and new systems	Incident response capabilities	Experience with transparency and explainability of AI solutions and clear documentation and reporting	Expertise in multi-cloud and hybrid identity management
Strategic planning for future scalability, transformation and cost management	Cloud migration and architecture design	Robust data privacy, security and risk management controls	Integration with next-generation AI systems and agentic workflows

In Closing

The shift from defend-and-block to get-hit-and-keep-going marks a substantial change in how organisations across Asia think about cyber resilience.

Regulations emphasising resiliency, surging data volumes, the weaponisation of AI, and the challenge of securing multi-infrastructure environments mean organisations must move beyond reactive incident response and invest strategically in defining their minimum viable company (MVC).

Yes, paying the ransom might work once, but repeatedly?

As the gap between business expectations for rapid recovery and operational reality drives organisations toward the false economy of ransom payments, the need for a well-defined MVC strategy becomes even more critical.

Commvault Perspective

The findings in this report reinforce a reality Commvault sees regularly across Asia: resilience is no longer a static capability or a point solution – it is an operating model. As accelerate AI adoption, expand data estates, and operate across increasingly complex hybrid and multi-cloud environments, resilience must be engineered into day-to-day operations, not bolted on after an incident.

This research highlights three areas where organisations must rethink how they prepare for and operate during disruption.

Minimum viability is now the foundation of cyber resilience

The shift towards a minimum viable company (MVC) mindset represents a fundamental change in how organisations approach cyber risk. The data shows that breaches are no longer an outlier event; they are an operational certainty. In this context, resilience is defined by how quickly and confidently an organisation can restore what matters most, not everything.

We see progressive organisations are the ones moving beyond traditional backup and recovery toward a cyber resilience platform approach that identifies, protects, and rapidly recovers the data, applications, and identities that underpin minimum viable operations.

Organisations that clearly define MVC – and those linking business priorities to recoverable technology capabilities – are far better positioned to keep the lights on, avoid ransom-driven decisions, and maintain trust with customers, regulators, and partners.

Closing the gap between business expectations and recovery reality requires a new operating model

This report again exposes a persistent disconnect: executives expect to be operational within days, while recovery in real-world environments still takes weeks. As data volumes grow, infrastructures fragment, and regulatory pressure increases. This gap becomes more dangerous – not just costly.

Closing it requires more than a better suite of tools. It requires ResOps: a resilience-first disciplinel that treats recovery, cyber response, and data protection as continuous, integrated functions. In a ResOps model, organisations unify security, IT operations, and data management around common visibility, automation, and recovery objectives. Clean data recovery, verified backups, rehearsed recovery playbooks, and AI-assisted orchestration are no longer emergency measures – they are standard operating practice.

Commvault sees ResOps as the natural evolution of SecOps and DevOps: an always-on discipline focused on operational survivability, not just incident response.

AI resilience and due diligence are critical to sustaining trust and value

AI is rapidly becoming embedded across business operations, IT, and cybersecurity. This research confirms both its promise and its risk. While AI can dramatically improve threat detection, recovery speed, and operational efficiency, rushing deployment without due diligence undermines resilience and trust.

From Commvault's perspective, AI resilience means ensuring AI systems, AI-generated data, and AI agents are protected, governed, and recoverable by design. Explainability, auditability, and compliance are prerequisites for safe adoption, not optional features. This is especially true as agentic AI introduces large numbers of non-human identities that operate autonomously across environments.

Resilient organisations apply consistent data and identity management principles across both human and machine actors, ensuring that AI augments cyber resilience without compromise. AI should strengthen ResOps by accelerating detection, validating recovery integrity, and automating response, while remaining transparent, controlled, and trustworthy.

In summary, this edition's research reinforces that readiness for the AI era is inseparable from resilience. Organisations that define minimum viability, operationalise recovery through ResOps, and adopt AI with discipline will be better equipped to withstand disruption and continue moving forward.

Commvault's cyber resilience platform is purpose-built to support this shift, bringing together data security, rapid recovery, identity awareness, and AI-driven automation at enterprise scale. This allows organisations to move from simply reacting to incidents to operating with confidence, even in the face of inevitable disruption.

Key Country Data Points


Korea
Philippines
Thailand
Malaysia

Key Country Data Points: Indonesia

This page summarises key data points from the commissioned survey.

Data growth in 12 months to 2026: 40%

Data infrastructure

- Hybrid: 20%
- Multi-cloud: 47%
- On-premises: 14%
- Single Cloud: 14%
- Other: 5%

Top 3 AI cybersecurity use cases

1. Improving threat detection speed and accuracy
2. Enhancing behavioural analytics and anomaly detection
3. Strengthening data privacy protection

Top 3 AI cybersecurity solution requirements

1. Integration with existing cybersecurity tools and workflows
2. Explainability and transparency of AI model decisions
3. Accuracy and speed of threat detection

How confident are you that your business can identify the following AI errors? 'Very high'

- Make a mistake: 39%
- Been compromised: 40%
- Broken GRC requirements: 45%
- Compromised data access guardrails: 44%

Has your organisation undertaken a thorough audit of security and GRC implications of AI solutions before they were deployed? 'Yes': 65%

Deployment of agentic AI (% trialling or adopted)

- IT operations: 36%
- Cybersecurity operations: 38%
- Business operations: 38%

Top 3 agentic AI challenges:

1. Ensuring appropriate access controls and privilege assignment for AI agents
2. Lack of visibility across distributed hybrid and multi-cloud environments
3. Integration difficulties between legacy identity systems and modern AI workflows

Incorporating human and non-human agent identity management into cyber resiliency plans. 'Yes, we have a strategy'

- Human: 84%
- Non-human: 43%

Have you been targeted by a ransomware attack? 'Yes': 60%

Top 3 ransomware payment considerations:

1. Expected speed of business recovery
2. Risk of permanent data loss if recovery unsuccessful
3. Confidence in the integrity and completeness of backups

Pay or not pay? 60% paid

Payment success? 'No': 45%

Defined MVB in your resiliency strategy and capabilities? 'Yes'

- Business operations: 81%
- Technology operations: 56%

Key Country Data Points: Hong Kong

This page summarises key data points from the commissioned survey.

Data growth in 12 months to 2026: 23%

Data infrastructure

- Hybrid: 21%
- Multi-cloud: 41%
- On-premises: 19%
- Single cloud: 15%
- Other: 4%

Top 3 AI cybersecurity use cases

1. Improving threat detection speed and accuracy
2. Enhancing behavioural analytics and anomaly detection
3. Strengthening data privacy protection

Top 3 AI cybersecurity solution requirements

1. Explainability and transparency of AI model decisions
2. Compliance with regulatory and reporting requirements
3. Integration with existing cybersecurity tools and workloads

How confident are you that your business can identify the following AI errors? 'Very high'

- Make a mistake: 40%
- Been compromised: 39%
- Broken GRC requirements: 37%
- Compromised data access guardrails: 39%

Has your organisation undertaken a thorough audit of security and GRC implications of AI solutions before they were deployed? 'Yes': 38%

Deployment of agentic AI (% trialling or adopted)

- IT operations: 36%
- Cybersecurity operations: 35%
- Business operations: 33%

Top 3 agentic AI challenges:

1. Ensuring appropriate access controls and privilege assignment for AI agents
2. Fragmented governance leading to inconsistent policies and oversight
3. Difficulty monitoring and auditing agentic AI activity across environments

Incorporating human and non-human agent identity management into cyber resiliency plans. 'Yes, we have a strategy'

- Human: 57%
- Non-human: 23%

Have you been targeted by a ransomware attack? 'Yes': 39%

Top 3 ransomware payment considerations:

1. Confidence in the integrity and completeness of backups
2. Potential reputational and legal risks associated with ransom payment
3. Total cost of each recovery path

Pay or not pay? 29% paid

Payment success? 'No': 44%

Defined MVB in your resiliency strategy and capabilities? 'Yes'

- Business operations: 64%
- Technology operations: 43%

Key Country Data Points: Korea

This page summarises key data points from the commissioned survey.

Data growth in 12 months to 2026: 29%

Data infrastructure

- Hybrid: 24%
- Multi-cloud: 44%
- On-premises: 11%
- Single Cloud: 12%
- Other: 9%

Top 3 AI cybersecurity use cases

1. Strengthening data privacy protection
2. Automating incident response and remediation
3. Improving threat detection speed and accuracy

Top 3 AI cybersecurity solution requirements

1. Explainability and transparency of AI model decisions
2. Compliance with regulatory and reporting requirements
3. Integration with existing cybersecurity tools and workloads

How confident are you that your business can identify the following AI errors? 'Very high'

- Make a mistake: 36%
- Been compromised: 27%
- Broken GRC requirements: 42%
- Compromised data access guardrails: 39%

Has your organisation undertaken a thorough audit of security and GRC implications of AI solutions before they were deployed? 'Yes': 31%

Deployment of agentic AI (% trialling or adopted)

- IT operations: 29%
- Cybersecurity operations: 36%
- Business operations: 34%

Top 3 agentic AI challenges:

1. Ensuring appropriate access controls and privilege assignment for AI agents
2. Difficulty monitoring and auditing agentic AI activity across environments
3. Integration difficulties between legacy identity systems and modern AI workflows

Incorporating human and non-human agent identity management into cyber resiliency plans. 'Yes, we have a strategy'

- Human: 57%
- Non-human: 22%

Have you been targeted by a ransomware attack? 'Yes': 36%

Top 3 ransomware payment considerations:

1. Risk of permanent data loss if recovery is unsuccessful
2. Total cost of each recovery path
3. Confidence in the integrity and completeness of backups

Pay or not pay? 31% paid

Payment success? 'No': 49%

Defined MVB in your resiliency strategy and capabilities? 'Yes'

- Business operations: 47%
- Technology operations: 32%

Key Country Data Points: Malaysia

This page summarises key data points from the commissioned survey.

Data growth in 12 months to 2026: 39%

Data infrastructure

- Hybrid: 21%
- Multi-cloud: 43%
- On-premises: 18%
- Single cloud: 12%
- Other: 6%

Top 3 AI cybersecurity use cases

1. Improving threat detection speed and accuracy
2. Enhancing behavioural analytics and anomaly detection
3. Strengthening data privacy protection

Top 3 AI cybersecurity solution requirements

1. Explainability and transparency of AI model decisions
2. Integration with existing cybersecurity tools and workloads
3. Accuracy and speed of threat detection

How confident are you that your business can identify the following AI errors? 'Very high'

- Make a mistake: 40%
- Been compromised: 48%
- Broken GRC requirements: 40%
- Compromised data access guardrails: 48%

Has your organisation undertaken a thorough audit of security and GRC implications of AI solutions before they were deployed? 'Yes': 38%

Deployment of agentic AI (% trialling or adopted)

- IT operations: 33%
- Cybersecurity operations: 32%
- Business operations: 31%

Top 3 agentic AI challenges:

1. Difficulty monitoring and auditing agentic AI activity across environments
2. Scale and lifecycle management of machine identities, keys and credentials
3. Lack of visibility across distributed hybrid and multi-cloud environments

Incorporating human and non-human agent identity management into cyber resiliency plans. 'Yes, we have a strategy'

- Human: 88%
- Non-human: 28%

Have you been targeted by a ransomware attack? 'Yes': 56%

Top 3 ransomware payment considerations:

1. Security of technical risks of re-infection or incomplete decryption
2. Expected speed of business recovery for each option
3. Risk of permanent data loss if recovery is unsuccessful

Pay or not pay? 29% paid

Payment success? 'No': 44%

Defined MVB in your resiliency strategy and capabilities? 'Yes'

- Business operations: 64%
- Technology operations: 43%

Key Country Data Points: Philippines

This page summarises key data points from the commissioned survey.

Data growth in 12 months to 2026: 40%

Data infrastructure

- Hybrid: 19%
- Multi-cloud: 40%
- On-premises: 19%
- Single Cloud: 9%
- Other: 14%

Top 3 AI cybersecurity use cases

1. Improving threat detection speed and accuracy
2. Strengthening data privacy protection
3. Enhancing behavioural analytics and anomaly detection

Top 3 AI cybersecurity solution requirements

1. Integration with existing cybersecurity tools and workloads
2. Accuracy and speed of threat detection
3. Explainability and transparency of AI model decisions

How confident are you that your business can identify the following AI errors? 'Very high'

- Make a mistake: 51%
- Been compromised: 50%
- Broken GRC requirements: 51%
- Compromised data access guardrails: 61%

Has your organisation undertaken a thorough audit of security and GRC implications of AI solutions before they were deployed? 'Yes': 60%

Deployment of agentic AI (% trialling or adopted)

- IT operations: 35%
- Cybersecurity operations: 35%
- Business operations: 30%

Top 3 agentic AI challenges:

1. Difficulty monitoring and auditing agentic AI activity across environments
2. Ensuring appropriate access controls and privilege assignments for AI agents
3. Integration difficulties between legacy identity systems and modern AI workflows

Incorporating human and non-human agent identity management into cyber resiliency plans. 'Yes, we have a strategy'

- Human: 83%
- Non-human: 49%

Have you been targeted by a ransomware attack? 'Yes': 54%

Top 3 ransomware payment considerations:

1. Confidence in the integrity and completeness of backups
2. Expected speed of business recovery for each option
3. Potential reputational and legal risks associated with ransom payment

Pay or not pay? 52% paid

Payment success? 'No': 29%

Defined MVB in your resiliency strategy and capabilities? 'Yes'

- Business operations: 74%
- Technology operations: 58%

Key Country Data Points: Singapore

This page summarises key data points from the commissioned survey.

Data growth in 12 months to 2026: 28%

Data infrastructure

- Hybrid: 27%
- Multi-cloud: 40%
- On-premises: 19%
- Single cloud: 9%
- Other: 6%

Top 3 AI cybersecurity use cases

1. Improving threat detection speed and accuracy
2. Enhancing behavioural analytics and anomaly detection
3. Strengthening data privacy protection

Top 3 AI cybersecurity solution requirements

1. Explainability and transparency of AI model decisions
2. Accuracy and speed of threat detection
3. Integration with existing cybersecurity tools and workloads

How confident are you that your business can identify the following AI errors? 'Very high'

- Make a mistake: 34%
- Been compromised: 45%
- Broken GRC requirements: 40%
- Compromised data access guardrails: 39%

Has your organisation undertaken a thorough audit of security and GRC implications of AI solutions before they were deployed? 'Yes': 23%

Deployment of agentic AI (% trialling or adopted)

- IT operations: 32%
- Cybersecurity operations: 32%
- Business operations: 33%

Top 3 agentic AI challenges:

1. Integration difficulties between legacy identity systems and modern AI workflows
2. Ensuring appropriate access controls and privilege assignment for AI agents
3. Inability to automate identity verification, rotation or deprovisioning

Incorporating human and non-human agent identity management into cyber resiliency plans. 'Yes, we have a strategy'

- Human: 67%
- Non-human: 29%

Have you been targeted by a ransomware attack? 'Yes': 32%

Top 3 ransomware payment considerations:

1. Confidence in the integrity and completeness of backups
2. Risk of permanent data loss if recovery is unsuccessful
3. Potential reputational and legal risks associated with ransom payment

Pay or not pay? 27% paid

Payment success? 'No': 46%

Defined MVB in your resiliency strategy and capabilities? 'Yes'

- Business operations: 70%
- Technology operations: 44%

Key Country Data Points: Thailand

This page summarises key data points from the commissioned survey.

Data growth in 12 months to 2026: 38%

Data infrastructure

- Hybrid: 20%
- Multi-cloud: 46%
- On-premises: 16%
- Single Cloud: 11%
- Other: 7%

Top 3 AI cybersecurity use cases

1. Improving threat detection speed and response
2. Automating incident response and remediation
3. Reducing manual workload and alert fatigue in SOC

Top 3 AI cybersecurity solution requirements

1. Integration with existing cybersecurity tools and workloads
2. Explainability and transparency of AI model decisions
3. Accuracy and speed of threat detection

How confident are you that your business can identify the following AI errors? 'Very high'

- Make a mistake: 43%
- Been compromised: 44%
- Broken GRC requirements: 55%
- Compromised data access guardrails: 53%

Has your organisation undertaken a thorough audit of security and GRC implications of AI solutions before they were deployed? 'Yes': 56%

Deployment of agentic AI (% trialling or adopted)

- IT operations: 35%
- Cybersecurity operations: 36%
- Business operations: 35%

Top 3 agentic AI challenges:

1. Scale and lifecycle management of machine identities, keys and credentials
2. Lack of visibility across hybrid and multi-cloud environments
3. Integration difficulties between legacy identity systems and modern AI workflows

Incorporating human and non-human agent identity management into cyber resiliency plans. 'Yes, we have a strategy'

- Human: 78%
- Non-human: 42%

Have you been targeted by a ransomware attack? 'Yes': 58%

Top 3 ransomware payment considerations:

1. Confidence in the integrity and completeness of backups
2. Expected speed of business recovery for each option
3. Risk of permanent data loss if recovery is unsuccessful

Pay or not pay? 55% paid

Payment success? 'No': 40%

Defined MVB in your resiliency strategy and capabilities? 'Yes'

- Business operations: 77%
- Technology operations: 53%

Key Country Data Points: Vietnam

This page summarises key data points from the commissioned survey.

Data growth in 12 months to 2026: 31%

Data infrastructure

- Hybrid: 21%
- Multi-cloud: 44%
- On-premises: 17%
- Single cloud: 14%
- Other: 6%

Top 3 AI cybersecurity use cases

1. Integration with existing cybersecurity tools and workloads
2. Explainability and transparency of AI model decisions
3. Compliance and regulatory reporting requirements

Top 3 AI cybersecurity solution requirements

1. Improving threat detection speed and accuracy
2. Enhancing behavioural analytics and anomaly detection
3. Automating incident response and remediation

How confident are you that your business can identify the following AI errors? 'Very high'

- Make a mistake: 34%
- Been compromised: 43%
- Broken GRC requirements: 46%
- Compromised data access guardrails: 49%

Has your organisation undertaken a thorough audit of security and GRC implications of AI solutions before they were deployed? 'Yes': 43%

Deployment of agentic AI (% trialling or adopted)

- IT operations: 34%
- Cybersecurity operations: 34%
- Business operations: 34%

Top 3 agentic AI challenges:

1. Integration difficulties between legacy identity systems and modern AI workflows
2. Difficulty monitoring and auditing agentic AI activity across environments
3. Lack of visibility across distributed hybrid and multi-cloud environments

Incorporating human and non-human agent identity management into cyber resiliency plans. 'Yes, we have a strategy'

- Human: 79%
- Non-human: 41%

Have you been targeted by a ransomware attack? 'Yes': 50%

Top 3 ransomware payment considerations:

1. Confidence in the integrity and completeness of backups
2. Expected speed of business recovery for each option
3. Total cost of each recovery path

Pay or not pay? 34% paid

Payment success? 'No': 35%

Defined MVB in your resiliency strategy and capabilities? 'Yes'

- Business operations: 70%
- Technology operations: 45%

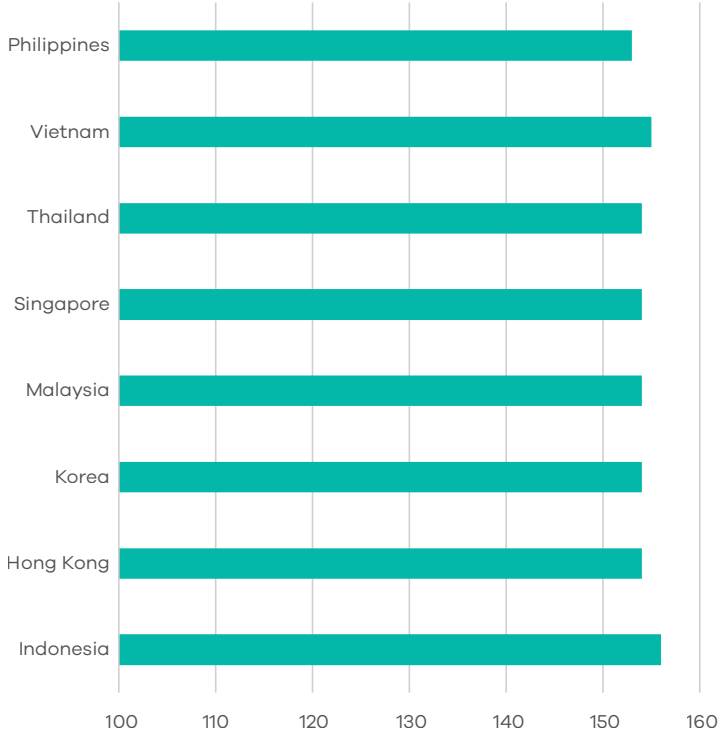
Appendix

The research methodology and demographics

Using an online panel, Tech Research Asia (now part of Omdia) conducted an independent quantitative market research survey in December 2025 and January 2026.

The total sample size is 1,234 organisations and respondents were CIO/CISO, IT leader, IT decision maker and direct reports.

All respondent companies were required to have between 100-199 or 200+ employees, each country had a 50/50 distribution between employee size groups.


Respondents by Country
Philippines
Vietnam
Thailand
Singapore
Malaysia
Korea
Hong Kong
Indonesia
100
110
120
130
140
150
160

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.

Omdia is a market-leading data, research, and consulting business focused on helping digital service providers, technology companies, and enterprise decision makers thrive in the connected digital economy. Through our global base of analysts, we offer expert analysis and strategic insight across the IT, telecoms, and media industries.

We create business advantage for our customers by providing actionable insight to support business planning, product development, and go-to-market initiatives.

Our unique combination of authoritative data, market analysis, and vertical industry expertise is designed to empower decision-making, helping our clients profit from new technologies and capitalize on evolving business models.

Omdia is part of Informa TechTarget, a B2B information services business serving the technology, media, and telecoms sector. The Informa group is listed on the London Stock Exchange.

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help your company identify future trends and opportunities.

Commvault®

Omdia by informa techtarget