SOPHOS

TRA

The Cybersecurity Playbook for Partners in Asia Pacific and Japan

A Tech Research Asia Report, commissioned by Sophos

September 2024

Introduction

This report is the 2nd of two e-books focused on the managed security partner (MSP) opportunity with cybersecurity in the Asia Pacific and Japan (APJ) markets of Australia, India, Japan, Malaysia, Singapore and the Philippines.

The first e-book:

1. Provided an overview of cybersecurity structures and teams, reporting lines and responsibilities
2. Pinpointed the key messages MSPs need to communicate to boards and executive leadership teams
3. Identified the key strategic pain points mid-market businesses have with cybersecurity in their operations
4. Revealed the hidden cybersecurity symptom undermining effective cybersecurity operations
5. Highlighted the common mistakes MSPs make when selling to businesses.

Key observations for partners from the first e-book include:

1. MSPs are considered critical to businesses' cybersecurity plans and operations
2. It's not quite one-size fits all, but a few sizes do suit many – there are similarities in how companies structure their cybersecurity groups, assign leaders and executive oversight
3. Boards and executive leadership teams are seeking guidance on key areas of interest – lean into these and provide insights
4. Technology is less of a problem than culture, burnout and education.

This second report analyses July 2024 research data into the cybersecurity needs of businesses in Australia, India, Japan, Malaysia, the Philippines and Singapore including:

1. The key links between business goals and cybersecurity investment
2. Visibility into cybersecurity budgets and areas of partner opportunity
3. The partner opportunities (and business concerns) for AI augmented cyber solutions
4. What businesses want from their cybersecurity partners
5. A perspective from report sponsor, Sophos, on the issues and partner opportunities
6. Individual country data snapshots from the research.

We hope the data and commentary in this TRA Playbook supports your go-to-market activities and ongoing commercial success.

Sincerely,

Tech Research Asia

The business need for cybersecurity

Many analyst authored playbooks start with an overview of the top business strategies and goals for the coming year.

This one does not.

Instead, we wanted to understand where companies see cybersecurity as critical to their business operations. Is it sales? Marketing? R&D? Logistics? Something else?

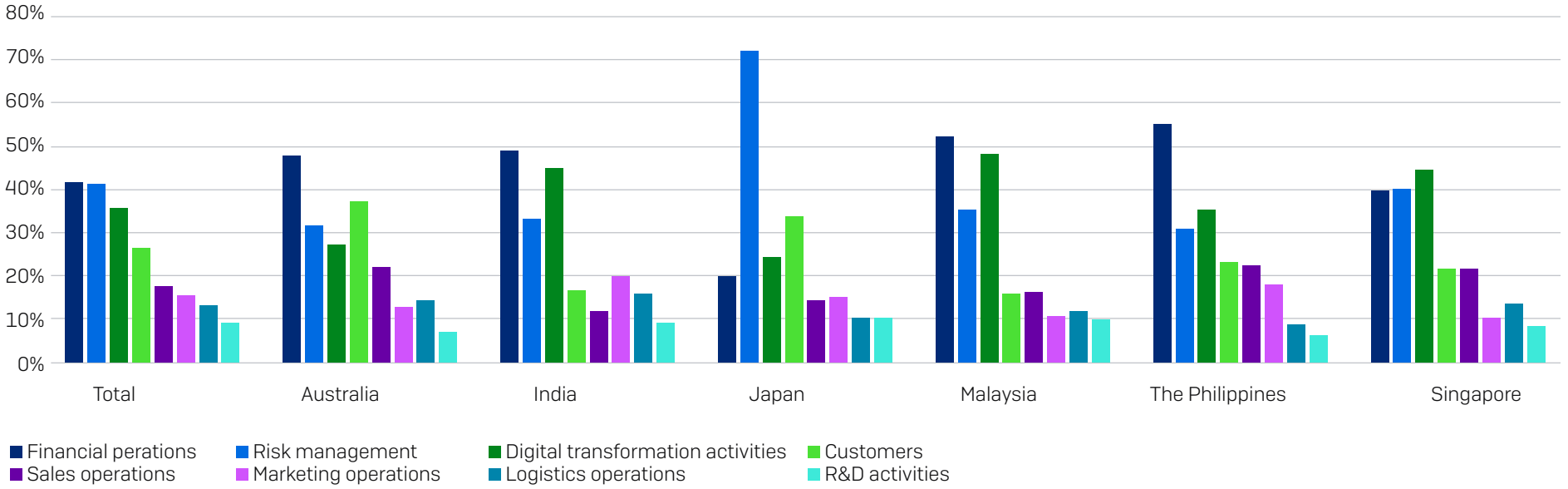
Across APJ, organisations told us that their top 3 areas of importance for cybersecurity and their business operations are:

1. Strengthening their cybersecurity posture around their **financial operations**
2. Improving their **risk management capabilities** and reducing their risk exposure
3. Ensuring the a robust cybersecurity platform is in place to **support digital transformation programs.**

Other key areas include:

- Strengthening protection of customers, their data, reducing phishing attacks, and improving customer communications and authentication
- Improving cyber resiliency for business operations, especially sales and customer support functions
- Protecting logistics and supply chains from cyber incidents and disruption and ensuring access to relevant operational data and systems in the event of an incident
- Preventing loss of company intellectual property and research and development data.

What are the top 3 most important business areas that require cybersecurity support?



Partner Cybersecurity Opportunity Heatmap

Which cybersecurity solutions do businesses view as important investment priorities?

Our 'Partner Cybersecurity Opportunity Heatmap' provides the answer. It illustrates which solutions are considered a high investment priority and the level of impact they have on an organisation's cybersecurity stance. The higher in the top right corner, the more important the solution.

The top 5 partner opportunities are:

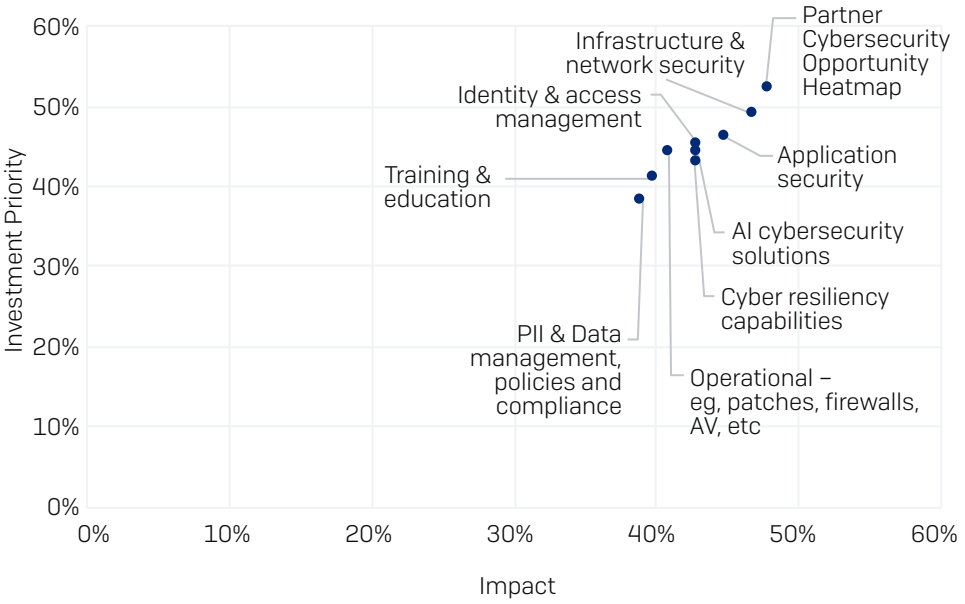
- Threat detection and response
- Infrastructure and network security
- Application security
- Identity and access management
- AI cybersecurity and cyber resiliency (equal 5th)

The first four solutions are well-established technologies and it's obvious that partners need to have strong credentials in these areas. More importantly, partners need to either develop, or continue strengthening, their capabilities in #5: AI-cybersecurity and cyber resiliency messaging.

Currently, 44% of businesses have an AI investment strategy for cybersecurity, and AI-cybersecurity will become table stakes (more on that later), underpinning many cybersecurity activities. Partners need to invest, build skills, hone messaging and go-to-market (GTM) activities, and build credibility or lose the opportunity to others.

Cyber resiliency messaging (maintaining business as usual during a cyber incident and recovery) is everywhere with many vendors positioning around it. With breaches regarded as inevitable by the majority of organisations, partners need a clear pitch around their resiliency capabilities. This includes supporting businesses with resiliency strategy development, board and senior leadership team education, and recovery planning.

Partner Cybersecurity Opportunity Heatmap



Note to the Heatmap:

Respondents were asked to rate the priority and impact of each technology solution on a scale of 0 (very low) to 10 (very high).

The Heatmap shows the percentage of respondents that selected 8,9, or 10 out of 10 for all countries.

Cybersecurity status and maturity

There are clear opportunities at both a product/solution level and strategy/frameworks for partners to help businesses boost their cybersecurity capabilities and maturity levels.

The data presented in the chart below represents the percentage of companies that have established security capabilities and strategies in place at both an aggregate and individual country level. The lower the percentage, the greater the potential opportunity for partners in that area.

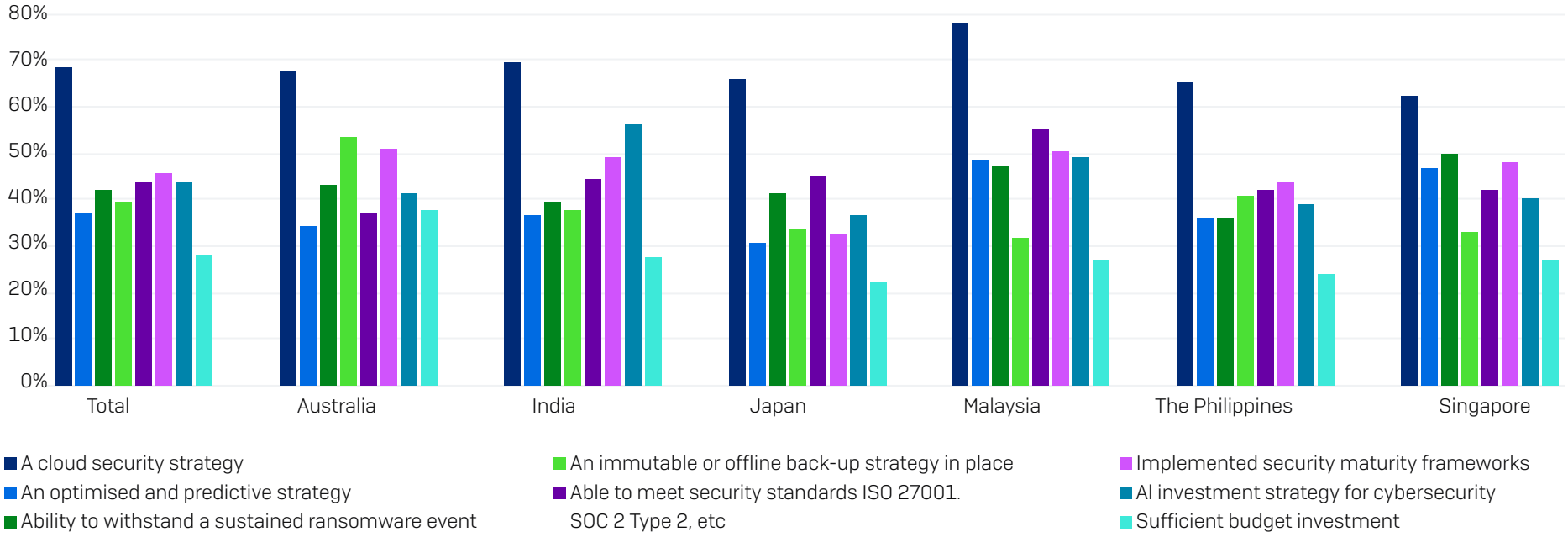
Budgets are clearly a pain point for many organisations, and we'll address this in more detail in the coming pages.

It's not just about the dollars though, partners need to have more than just product solutions to offer customers.

There is a distinct requirement for partners to support a number of strategy and framework needs including:

1. Building stronger maturity through helping businesses optimise their cybersecurity strategies and ability to withstand ransomware (and other) attacks
2. Providing insights and education on establishing and implementing security maturity frameworks
3. Supporting companies to attain and keep multiple security standards certifications
4. Helping companies establish and maintain zero trust cybersecurity strategies and operations.

Of the security capabilities identified as important to your organisation, which of the following do you currently have in place?



Budgets. How much and where?

There's good news on budgets for partners.

On average, 72% of companies in APJ state they do not have enough budget currently allocated to cybersecurity and 83% of Asia Pacific organisations expect to have their cybersecurity budget increase in the next 12 months.

For those companies increasing their spend on cybersecurity, 21% expect an increase of more than 10%.

Linking back to our earlier commentary on the top heat map priorities, the top product and solution areas attracting higher budgets are:

1. Infrastructure and network security (62% are increasing budgets)
2. Threat detection and response/data protection and privacy (61% are increasing budgets)
3. Application security (56% are increasing budgets)
4. Identity access management (53% are increasing)
5. Incident response and recovery (50% are increasing).

Other areas earmarked for substantial increases include:

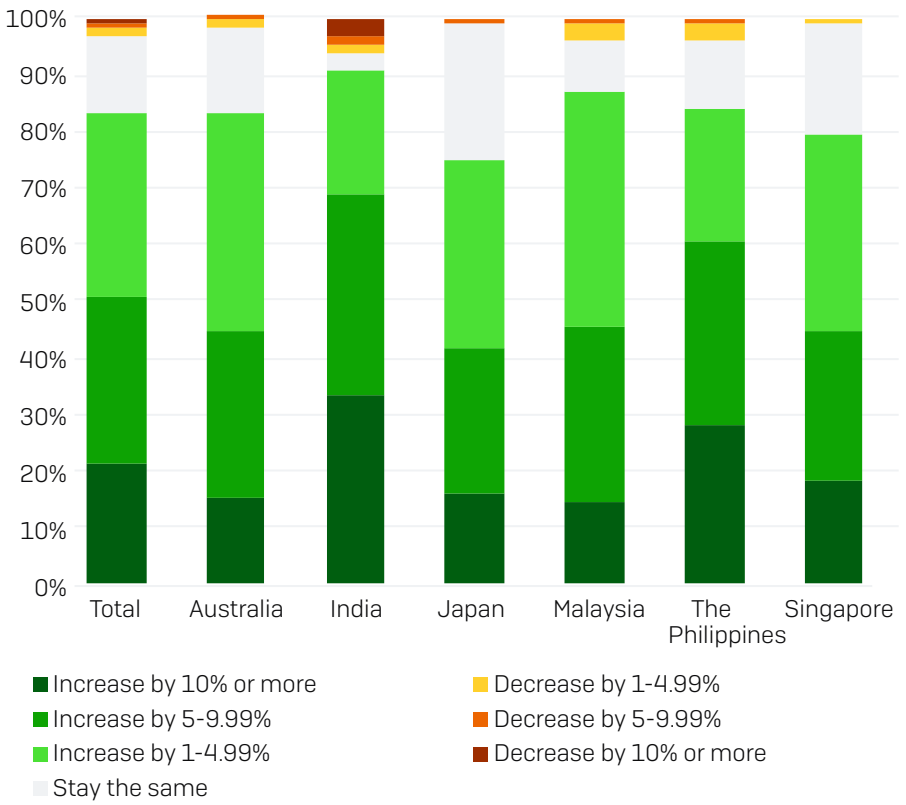
1. Data protection and privacy policies and strategy (62% are increasing)
2. Training and education programs (56% are increasing),
3. Cybersecurity strategy, talent and governance, risk and compliance activities (55% are increasing)
4. Insurance (48% are increasing).

Companies are also planning to invest more with in-house employees, with 50% of organisations planning to increase their salary budget line item.

Unsurprisingly, with the increase in salaries there is a need to look at cost-effective alternatives. 50% of companies have indicated they intend to invest in more third-party managed security services.

Of those increasing their third-party spending, 20% expect to see this grow by more than 10%, the remaining 80% by 1-10%.

Will your company's cybersecurity budget increase or decrease in the coming 12 months?



Demand for Partner Engagement is Strong

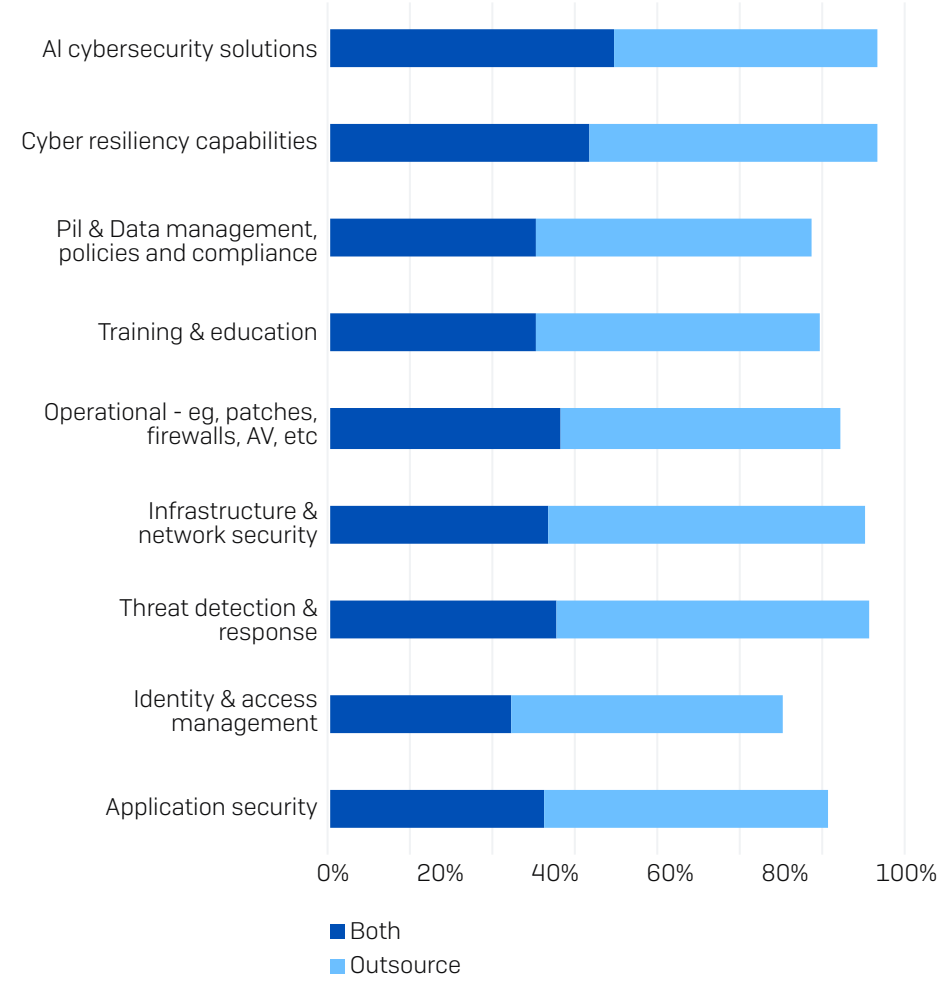
The data shows organisations are willing to work with partners, recognising a number of benefits including:

- Consolidation and management of multiple infrastructure, end-point environments and toolsets,
- Managed SOC services that enhance security capabilities and reduce impact on in-house employees,
- Alleviating in-house skills shortages,
- Ensuring basic activities such as credential management, patching, etc are up-to-date,
- Addressing budget concerns through cost-effective third party services rather than more expensive in-house employees, and
- Addressing the focus on risk reduction and mitigation through governance, risk and compliance audits, assessment and management.

The chart to the right shows the current demand for third party support (outsourced) or both (mix of in-house and outsourced support) in a number of cybersecurity areas, clearly indicating robust demand for partners.

Looking forward over the coming 2 years, the intent to outsource remains strong and relatively constant. Two areas showing an increase in outsourced demand, namely application security and PII & data management, policies and compliance services.

Which of the following cybersecurity requirements does your company currently do in-house, outsource or mix of both? (Note chart does not show 'in-house')



Threat concerns: It starts with AI

AI is a key topic in almost every business technology discussion. In all markets except Australia, AI-augmented cybersecurity attacks are considered the most worrying cyber threat for organisations.

Partners must have clear talk tracks that address the reality of threat actors using AI-augmented attacks, the AI-strategies and capabilities that the partner's vendors have in place, supported by 'where to start with cyber and AI' go-to-market messaging and campaigns. This is not just about product – it extends to AI policy, ethics, acceptable usage and user access and management.

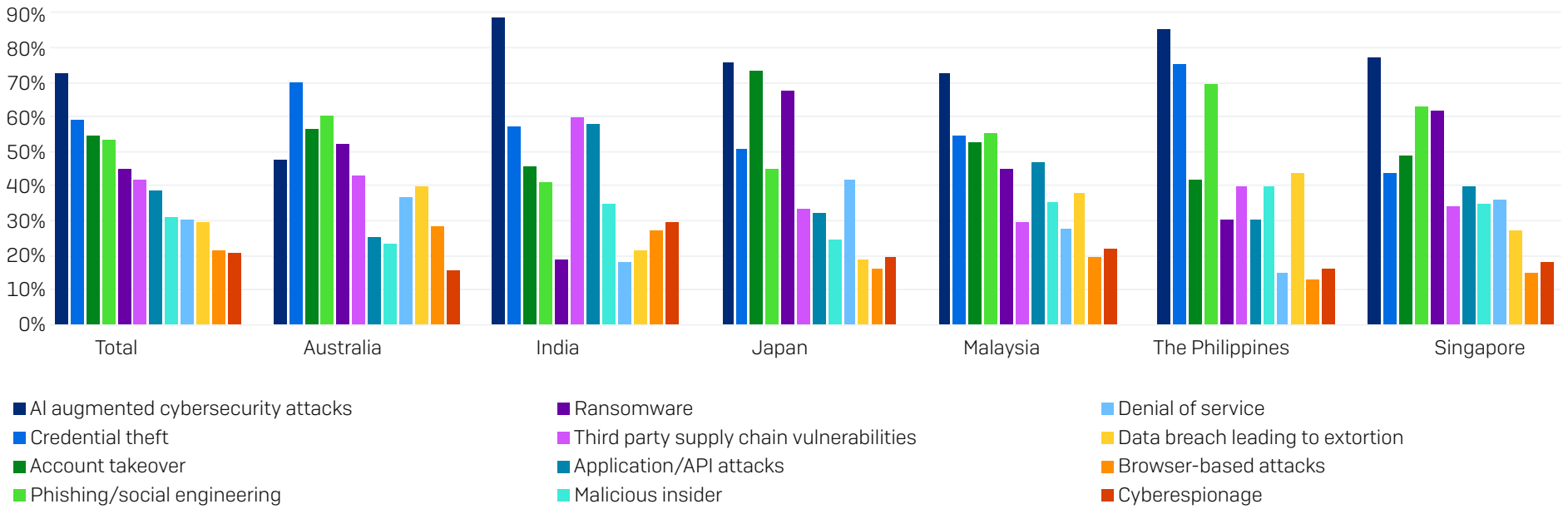
Selling AI fear, uncertainty and doubt (FUD) will not cut it.

Selling skills, competency and capabilities will: Currently less than half of APJ organisations think they have all the necessary skills to deal with the threat of AI-augmented attacks.

Across the region, 45% of companies believe they have the skills to deal with an AI threat. This creates clear prospects for partners to engage and support organisations – both from a managed security perspective as well as training and education.

Apart from AI-augmented threats, concerns vary widely across different countries and for partners understanding the core threats for your target market is a key. Even more so if you're targeting multiple countries as part of your operations.

"Which of the following cyber threats do you worry about the most?"



The broader AI cybersecurity opportunity

Approached in the right way, partners have considerable revenue opportunities supporting organisations as they adopt and deploy AI cybersecurity solutions.

Start with the strategy. Today, only 22% of organisations say they have a comprehensive AI and automation strategy in place across the organisation. There is a clear need to help businesses wade through the morass of AI content and confusion.

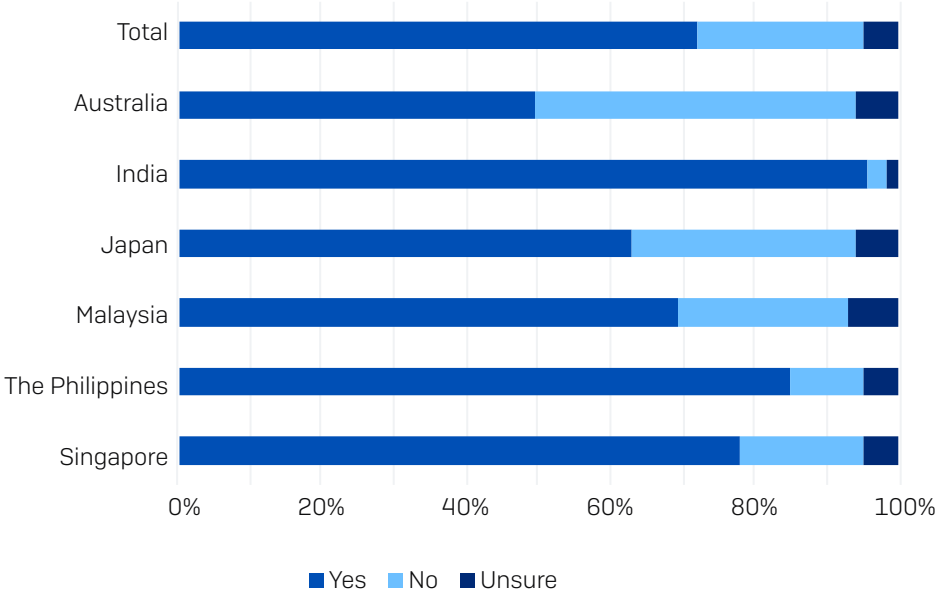
Move quickly. Companies are already progressing their AI cybersecurity strategies:

- 72% report they have appointed a person to lead the AI strategy and initiatives. Not all these leaders are technologists. In fact 3/4s will typically be line of business executives (sales, marketing, finance, etc) – business outcome discussions trump tech pitches.
- 75% have already spoken with their existing partner about AI-related cybersecurity, (however only 26% scored their current partner 5 out of 5 on their AI cybersecurity skills and knowledge).
- 8% have already moved to a different partner as a result.

Business AI skills shortages are a clear win for partners. To deal with AI skills shortages, 45% will outsource to partners to support. 49% intend to train and develop in-house skills and will require partner supported training and education.

Help organisations get 'AI-fit'. TRA research indicates that companies move through three distinct AI phases – strategy, ideation and deploy/run. To optimise stage three (deploy/run), companies need to audit their networks, storage, end-points, GRC and security and data estates to assess their AI-readiness. Partners have a clear role to play here.

Does your organisation have a clearly appointed person to lead your AI strategy and initiatives?



What business want from partners

This part of the playbook sets out a number of factors impacting an organisation's decision to use third-party organisations to support their cybersecurity needs and operations.

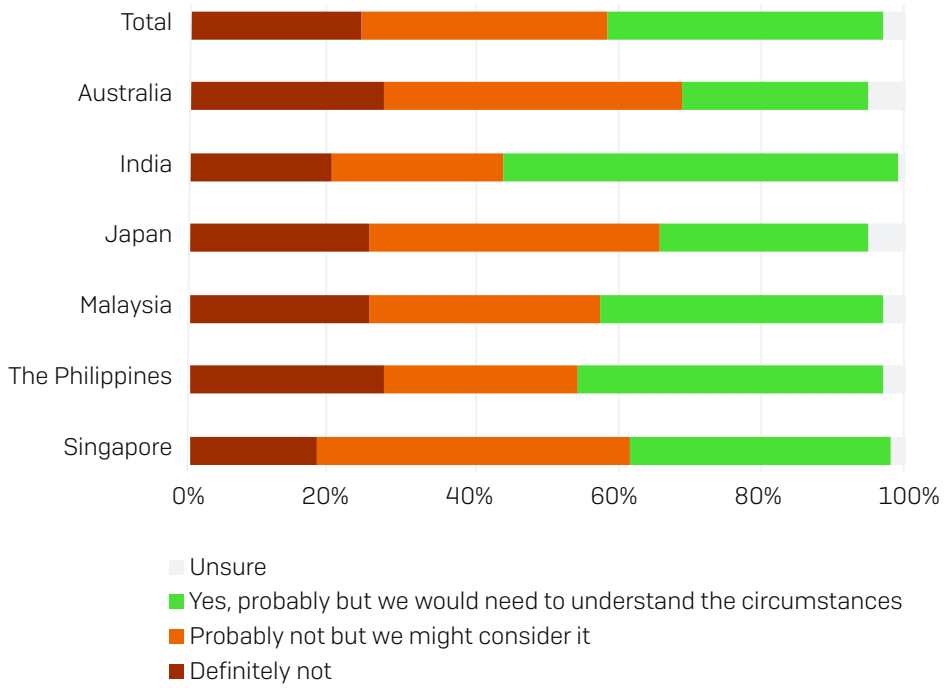
Before we get to these, there are, of course, some basics that partners should have in place including:

- Credible, industry leading vendor agreements and reputation
- Integration skills
- Proactive threat detection capabilities
- Cyber resiliency capabilities and expertise,
- Use of, and support for, AI-augmented cybersecurity solutions
- Ability to tailor solutions to specific customer needs
- Education and training support.

Strong partner security skills are a must. While we know that's stating the very obvious, the data makes it very clear: 59% of organisations will 'definitely' or 'probably' not engage a partner that had been breached or suffered a security incident.

And for partners that were breached and are still in consideration, expect to be subject to tighter terms – 81% of companies that would consider a breached partner will include extra performance clauses and specific service level agreements.

Would your organisation sign a contract with a third party that had experienced a cybersecurity incident, breach or loss of data in the last 12 months?



It's not just you.

Multi-vendor environments are a way of life.

On average, 20% of organisations use just one vendor for their cybersecurity needs. 29% use two, another 23% use three and 10% use five or more vendor solutions.

Making sure your commercial constructs are flexible and tailored to customer needs is imperative:

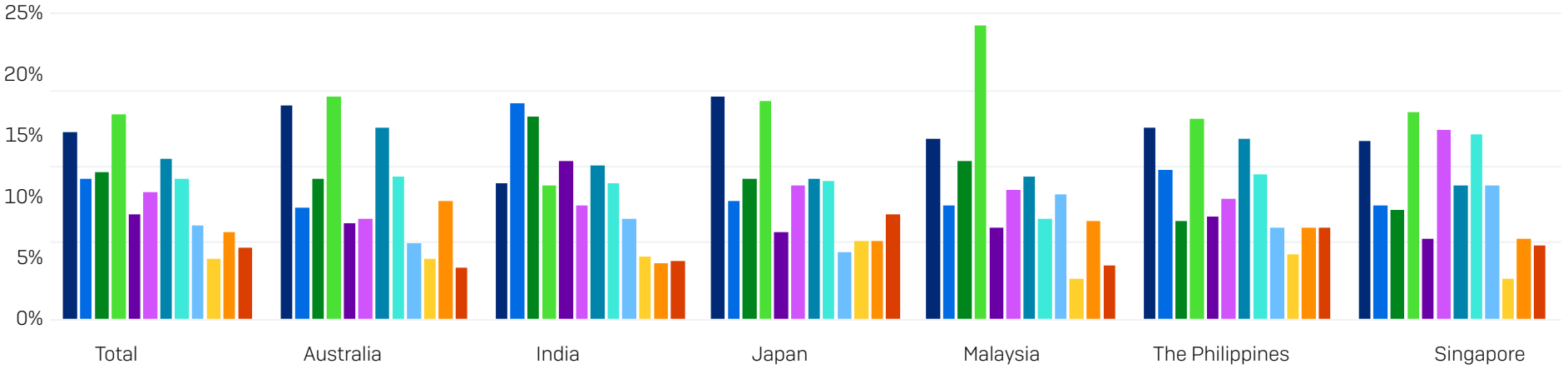
- 54% of organisations want outcomes-based terms as part of their contracts in the next 24 months
- 48% want pricing that combines consumption-based and fixed contracts, 31% prefer fixed terms and 17% want consumption-based pricing only.

The top 3 reasons given for considering a change in cybersecurity vendor or strategy are:

1. Poor performance of the solution
2. A breach or major outage 3rd parties with data and systems access
3. Budget change

Tight budgets and business cost optimisation demands are an opportunity for those partners than can demonstrate flexible commercial models and unified platforms and toolsets that reduce management and education costs.

Excluding pricing, what factors would make you consider a change of cybersecurity vendor or strategy?



Marketplaces a comment

From our research and conversations with APJ channel organisations and distributors, we know marketplaces can be problematic for many partners. Margins are ultra-low and incumbency protection is challenging.

We also know that organisations intend to continue using marketplaces to buy and consume cybersecurity solutions.

Partners competing head-to-head with marketplaces on price to win a customer's business will typically lose. Cloud commercials, especially committed cloud credits, simply make it too hard.

Instead, there are several factors partners can build into their value proposition and engagements to mitigate the marketplace malaise including:

- **Risk management #1.** Emphasising that whilst marketplaces are acceptable for simple, do-it-yourself (DIY), stand-alone deployments, many cybersecurity engagements are complex, require integration and multi-platform support. With a focus on risk management and reduction as part of core business needs, companies need partner support to ensure a robust risk posture and cybersecurity capability.
- **Risk management #2.** Marketplace DIY purchases without proper due diligence on product performance and capabilities create higher risk and there can be issues with responsibility with cyber incidents if an organisation has deployed part of a solution and a partner the other.
- **Professional services add-ons** are a strong option to bring additional value and customer stickiness over the top of marketplace procurement. These also help to accelerate the realisation of value from the investment, a key consideration in today's cost-conscious environment.

In closing

Demand for managed security partner support is strong

83% of companies indicated cybersecurity budgets will increase in the coming 12 months, and 50% also stated they will increase their spend with MSPs over the same period.

Increasingly companies are looking to partners for cybersecurity with a serve of cyber resiliency capabilities. This means MSPs need to present strong technical cybersecurity skills as well as a clear understanding of their customers' business goals and operations.

Threat detection and response, infrastructure and network security, application security, IAM, cyber resiliency and (defensive and offensive) AI cybersecurity are clearly identified as areas of technical demand.

To drive deeper and stickier engagement, partners clearly link these technical skills to protecting customer data (and brand reputation), financial operations, sales, marketing, digital transformation, etc all while maintaining business as (almost) usual during attacks or breaches.

Even better if you can clearly and practically explain the real importance of AI cybersecurity operations, and perhaps more importantly, the impact that adopting AI tools in business (such as generative AI) and IT operations has on an organisations cybersecurity and risk profiles.

Eliminate the FUD selling, concentrate on credibility, skills and execution capabilities to win the business

Businesses are bombarded with nonstop cybersecurity tools promising a nirvana-like end state of total protection. They're over it. Selling on fear, uncertainty and doubt (FUD) isn't effective.

Instead, concentrate on your credibility, the depth of your vendor partnerships and their reputations, integration skills, practical proof points of execution and value, and education and training of employees. These are the messages that companies told us resonate positively with both their technology and business teams (and buyers).

Finally, we have provided individual snapshots to provide specific data points for businesses in each of the six countries we researched.

The SOPHOS Perspective

Successful MSPs build enduring partnerships with their customers

The data is clear. Businesses are willing to outsource services. However, most are looking for a hybrid model comprising inhouse resources and outsourced services. This is why the partners that succeed don't just provide services but invest in building and maintaining enduring partnerships with their customers. This includes having a focus on working with internal staff, not replacing them.

This research from TRA provides valuable insights and data drawn directly from the market highlighting the business areas that matter most to customers. I urge MSPs to take advantage of these insights and the key takeaways provided by TRA to focus their efforts and messaging. With 50% of companies indicating they intend to invest in more third-party managed security services, now's the perfect time for MSPs to consider how they are offering cybersecurity as a service to their customers and prospects.

MSPs can provide businesses regardless of their size with the best defences against the constantly evolving threat landscape. Using this eBook and its predecessor as a guide, MSPs should look to partner with a vendor that provides the depth of services required to take advantage of this unique opportunity in a profitable way that minimises overheads and risks.

For more information, please visit: www.sophos.com

Country data snapshot - Australia

Top business areas needing cybersecurity support:

1. Financial services
2. Customers
3. Risk management
4. Digital transformation
5. Marketing services

Number of cybersecurity vendor solutions used:

1: 29%
2: 25%
3: 23%
4: 3%
5+: 2%
Unsure: 18%

Comprehensive AI adoption strategy in place:

10%

AI leader appointed:

50%

Do you have the necessary AI skills in-house?

"Yes" 28%

How do you rate your preferred partner's AI knowledge?

5-out-of 5: 15%
4-out-of-5: 47%

Would you use a partner that had experienced a cyber incident?

"Definitely not" 27%

"Probably not" 41%

Would you impose higher performance and SLAs on a breached partner?

"Yes" 60%

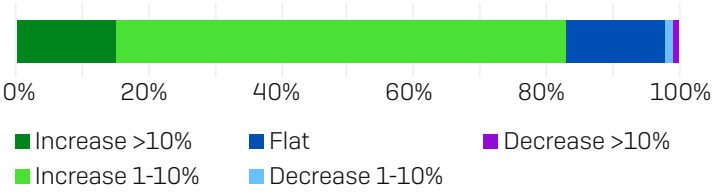
Why change cybersecurity vendors?

1. Poor solution performance
2. We were breached
3. Too complex to manage
4. Poor penetration testing results
5. Poor technical support

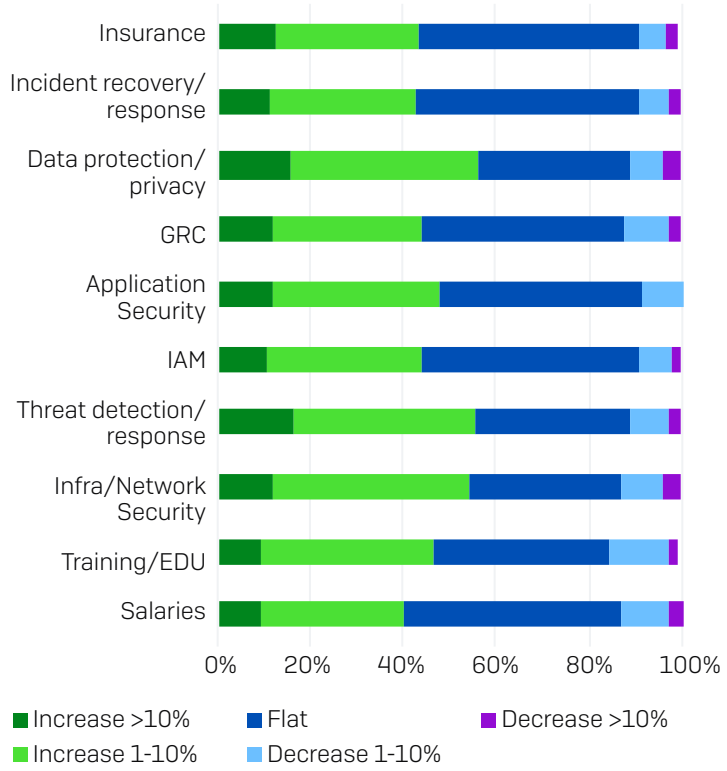
Relevant frameworks

- Australian Signals Directorate (ASD) Information Security Manual (ISM)
- Australian Cybersecurity Centre Essential 8
- (US) National Institute of Standards & Technology (NIST) Cyber Security Framework
- ISO 27001 and ISO 27002
- Cloud Security Alliance (CSA) Cloud Control Matrix (CCM

Expected budget change:



Expected budget line item changes:



Country data snapshot - India

Top business areas needing cybersecurity support:

1. Financial services
2. Digital transformation
3. Risk management
4. Marketing operations
5. Customers

Number of cybersecurity vendor solutions used:

1: 5%
2: 25%
3: 24%
4: 21%
5+: 26%
Unsure: 1%

Comprehensive AI adoption strategy in place:

38%

AI leader appointed:

96%

Do you have the necessary AI skills in-house?

"Yes" 72%

How do you rate your preferred partner's AI knowledge?

5-out-of 5: 49%
4-out-of-5: 44%

Would you use a partner that had experienced a cyber incident?

"Definitely not" 20%
"Probably not" 24%

Would you impose higher performance and SLAs on a breached partner?

"Yes" 98%

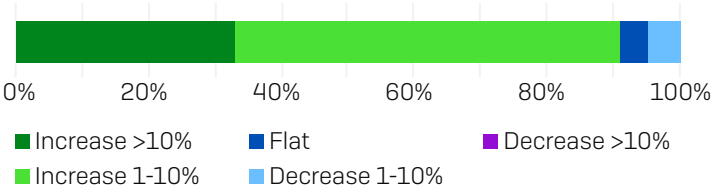
Why change cybersecurity vendors?

6. Vendor supply chain problems
7. Poor solution performance
8. Vendor changes staff/representatives
9. Budget change
10. Too complex to manage

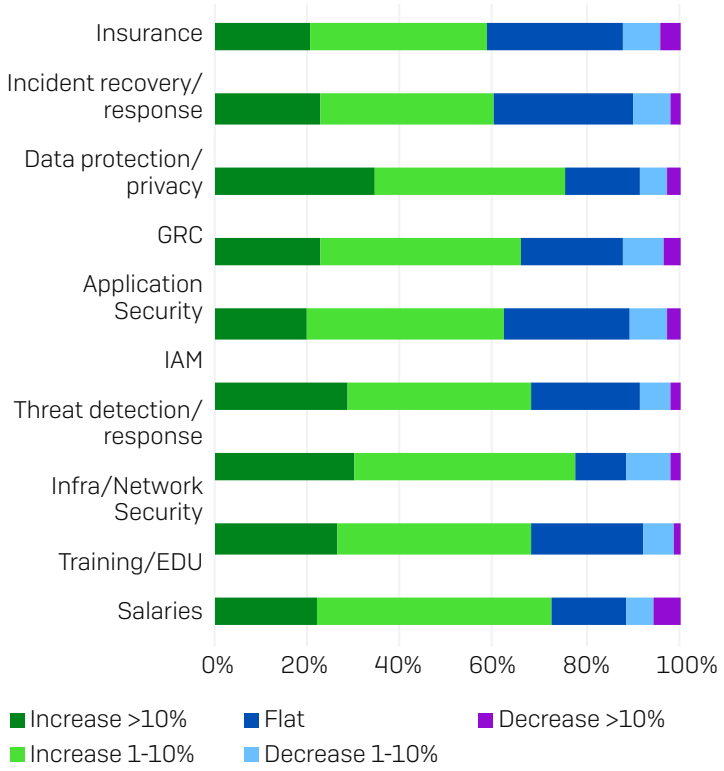
Relevant frameworks

- Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013
- Information Technology (Information Security Practices and Procedures for Protected System) Rules, 2018
- The Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code Rules, 2021)
- (US) National Institute of Standards & Technology (NIST) Cyber Security Framework
- ISO 27001 and ISO 27002
- Cloud Security Alliance (CSA) Cloud Control Matrix (CCM

Expected budget change:



Expected budget line item changes:



Country data snapshot - Japan

Top business areas needing cybersecurity support:

1. Risk management
2. Customers
3. Digital transformation
4. Financial operations
5. Sales

Number of cybersecurity vendor solutions used:

1: 23%
2: 31%
3: 24%
4: 2%
5+: 4%
Unsure: 14%

Comprehensive AI adoption strategy in place:

15%

AI person appointed:

63%

Do you have the necessary AI skills in-house?

"Yes" 30%

How do you rate your preferred partner's AI knowledge?

5-out-of 5: 9%
4-out-of-5: 54%

Would you use a partner that had experienced a cyber incident?

"Definitely not" 25%
"Probably not" 41%

Would you impose higher performance and SLAs on a breached partner?

"Yes" 74%

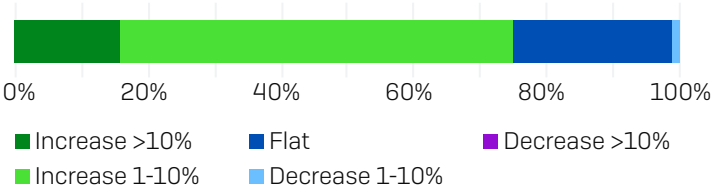
Why change cybersecurity vendors?

1. We were breached
2. Poor performance
3. Too complex to manage
4. Poor penetration testing results
5. Poor technical support

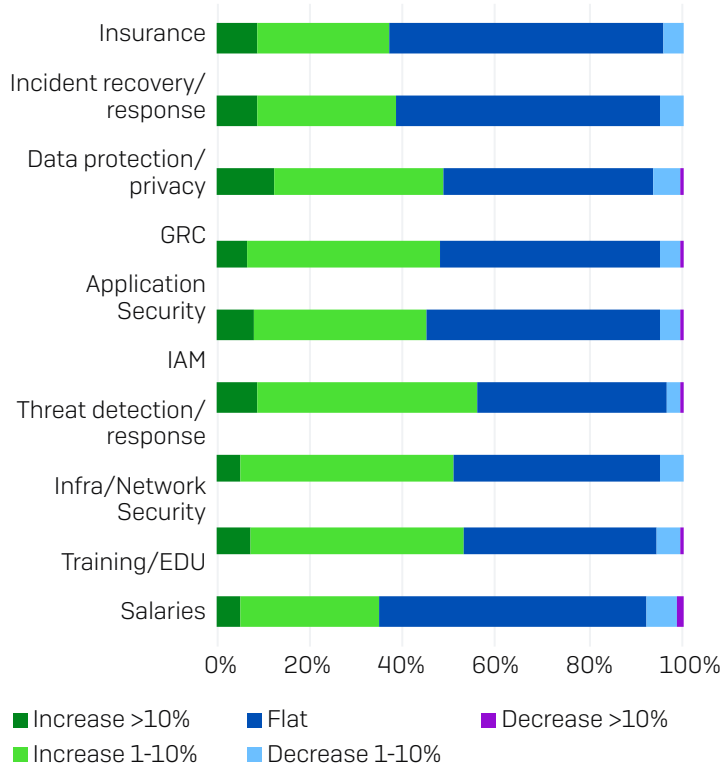
Relevant frameworks

- National Center of Incident Readiness and Strategy for Cybersecurity (NISC) - Common Standards Group for Cybersecurity Measures for Government Agencies and Related Agencies
- Guidelines for the Formulation of Information Security Policies, 2021 edition
- (US) National Institute of Standards & Technology (NIST) Cyber Security Framework
- ISO 27001 and ISO 27002
- Cloud Security Alliance (CSA) Cloud Control Matrix (CCM

Expected budget change:



Expected budget line item changes:



Country data snapshot - Malaysia

Top business areas needing cybersecurity support:

1. Financial services
2. Digital transformation
3. Risk management
4. Customers
5. Sales

Number of cybersecurity vendor solutions used:

1: 25%
2: 29%
3: 25%
4: 12%
5: 5%
Unsure: 4%

Comprehensive AI adoption strategy in place:

15%

AI leader appointed:

46%

Do you have the necessary AI skills in-house?

"Yes" 46%

How do you rate your preferred partner's AI knowledge?

5-out-of 5: 20%
4-out-of-5: 56%

Would you use a partner that had experienced a cyber incident?

"Definitely not" 25%
"Probably not" 32%

Would you impose higher performance and SLAs on a breached partner?

"Yes" 86%

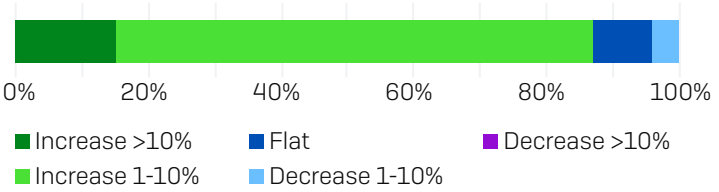
Why change cybersecurity vendors?

1. Poor solution performance
2. We were breached
3. Poor penetration testing results
4. Budget change
5. Too complex to manage

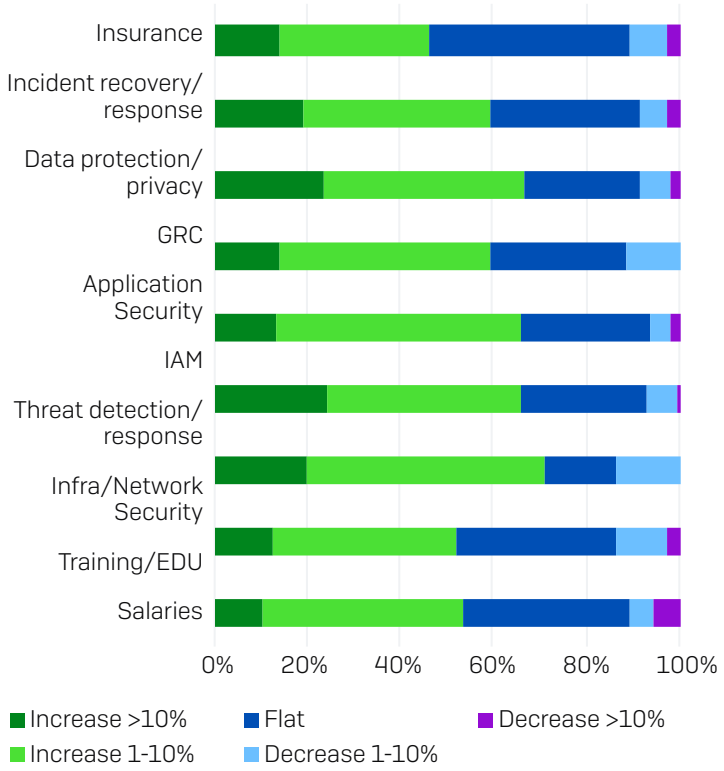
Relevant frameworks

- Malaysian Government Cyber Security Bill 2024
- Malaysian Cyber Security Framework For Public Sector (RAKKSSA)
- (US) National Institute of Standards & Technology (NIST) Cyber Security Framework
- ISO 27001 and ISO 27002
- Cloud Security Alliance (CSA) Cloud Control Matrix (CCM

Expected budget change:



Expected budget line item changes:



Country data snapshot – The Philippines

Top business areas needing cybersecurity support:

1. Financial services
2. Customers
3. Risk management
4. Digital transformation
5. Marketing services

Number of cybersecurity vendor solutions used:

1: 20%
2: 27%
3: 21%
4: 10%
5: 17%
Unsure: 6%

Comprehensive AI adoption strategy in place:

36%

AI leader appointed:

85%

Do you have the necessary AI skills in-house?

"Yes" 59%

How do you rate your preferred partner's AI knowledge?

5-out-of 5: 41%
4-out-of-5: 48%

Would you use a partner that had experienced a cyber incident?

"Definitely not" 28%
"Probably not" 27%

Would you impose higher performance and SLAs on a breached partner?

"Yes" 93%

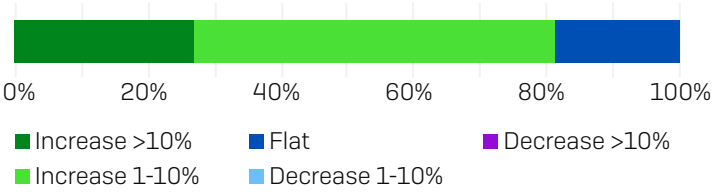
Why change cybersecurity vendors?

1. Poor solution performance
2. We were breached
3. Budget change
4. Vendor supply chain problems
5. Penetration testing results

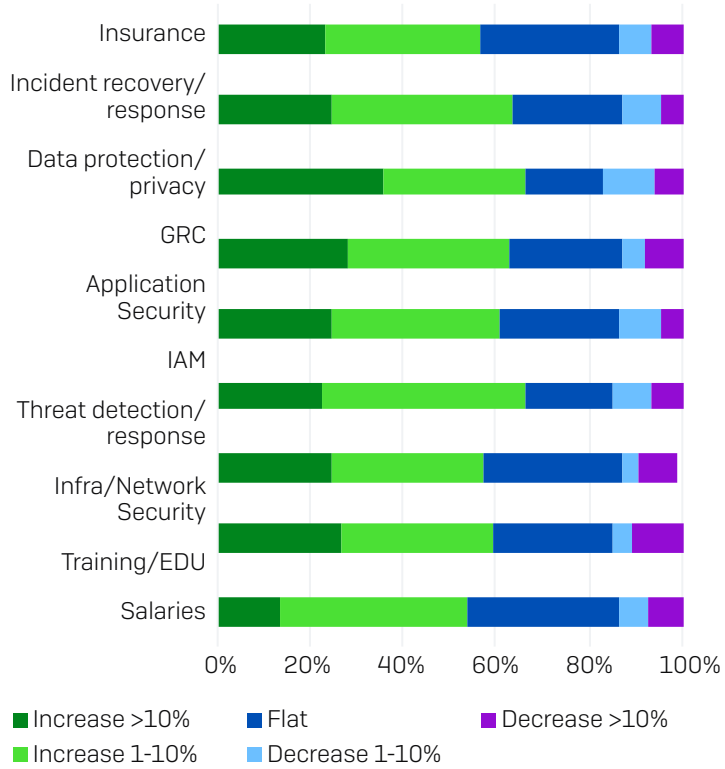
Relevant frameworks

- Department of Information and Communications Technology (DICT) National Cybersecurity Plan (NCSP) 2023-2028
- (US) National Institute of Standards & Technology (NIST) Cyber Security Framework
- ISO 27001 and ISO 27002
- Cloud Security Alliance (CSA) Cloud Control Matrix (CCM

Expected budget change:



Expected budget line item changes:



Country data snapshot - Singapore

Top business areas needing cybersecurity support:

1. Digital transformation
2. Financial services
3. Risk management
4. Sales
5. Customers

Number of cybersecurity vendor solutions used:

1: 24%
2: 40%
3: 18%
4: 8%
5: 7%
Unsure: 4%

Comprehensive AI adoption strategy in place:

24%

AI leader appointed:

43%

Do you have the necessary AI skills in-house?

"Yes" 28%

How do you rate your preferred partner's AI knowledge?

5-out-of 5: 20%

4-out-of-5: 55%

Would you use a partner that had experienced a cyber incident?

"Definitely not" 18%
"Probably not" 44%

Would you impose higher performance and SLAs on a breached partner?

"Yes" 83%

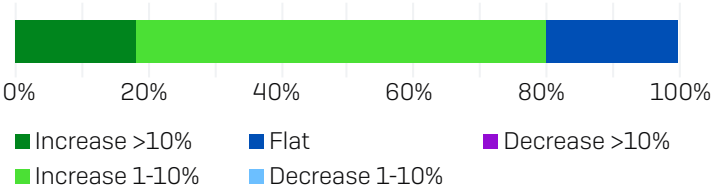
Why change cybersecurity vendors?

1. Poor solution performance
2. We were breached
3. Regulatory or legislative changes
4. Poor solution performance
5. Too complex to manage

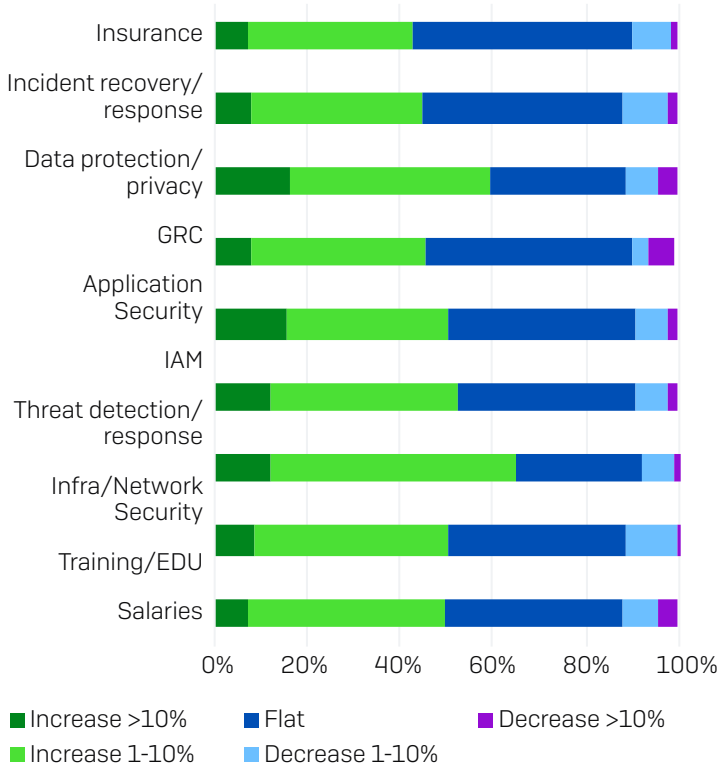
Relevant frameworks

- Cyber Security Agency of Singapore (SINGCert) Cybersecurity Act
- SINGCert Cyber Essentials
- (US) National Institute of Standards & Technology (NIST) Cyber Security Framework
- ISO 27001 and ISO 27002
- Cloud Security Alliance (CSA) Cloud Control Matrix (CCM

Expected budget change:



Expected budget line item changes:



About

Data referenced in this report is drawn from TRA's research for Sophos conducted in July 2024 from a sample of 900 companies across Australia, India, Japan, Malaysia, Philippines & Singapore.

ABOUT SOPHOS. Sophos is a global leader and innovator of advanced security solutions for defeating cyberattacks, including Managed Detection and Response (MDR) and incident response services and a broad portfolio of endpoint, network, email, and cloud security technologies. As one of the largest pure-play cybersecurity providers, Sophos defends more than 600,000 organizations and more than 100 million users worldwide from active adversaries, ransomware, phishing, malware, and more. Sophos' services and products connect through the Sophos Central management console and are powered by Sophos X-Ops, the company's cross-domain threat intelligence unit. Sophos X-Ops intelligence optimizes the entire Sophos Adaptive Cybersecurity Ecosystem, which includes a centralized data lake that leverages a rich set of open APIs available to customers, partners, developers, and other cybersecurity and information technology vendors. Sophos provides cybersecurity-as-a-service to organizations needing fully managed security solutions. Customers can also manage their cybersecurity directly with Sophos' security operations platform or use a hybrid approach by supplementing their in-house teams with Sophos' services, including threat hunting and remediation. Sophos sells through reseller partners and managed service providers (MSPs) worldwide. Sophos is headquartered in Oxford, U.K. More information is available at www.sophos.com.

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

2024-09-06 (WP-NP)

SOPHOS