The Partner Opportunity with Cybersecurity in Asia Pacific

A Tech Research Asia Insights Report, commissioned by Sophos

May 2024

SOPHOS

TRA

Introduction

This report is #the first of a 2-part series focused on the managed security partner (MSP) opportunity with cybersecurity in the Asia Pacific markets of Australia, India, Japan, Malaysia, Singapore and the Philippines.

This e-book:

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

The second e-book will provide insights for MSPs into:

1. The total addressable market for cybersecurity solutions in the small and medium business sector
2. Cybersecurity spending indicators and key budget stakeholders
3. A heatmap of business cybersecurity investment priorities for the coming 12 months
4. The 'outsource, inhouse or mixture of both' approach businesses want cybersecurity products and solutions.

Key observations for partners 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.

We hope the data and commentary in this Insights Report augments your own go-to-market activities and supports ongoing commercial success.

Sincerely,

Tech Research Asia

SOPHOS

TRA

Navigating cybersecurity structures

Having cybersecurity operations is a clear focus for 98% of all businesses surveyed (and we'd assume the 2% that don't won't be around for too much longer anyway...)

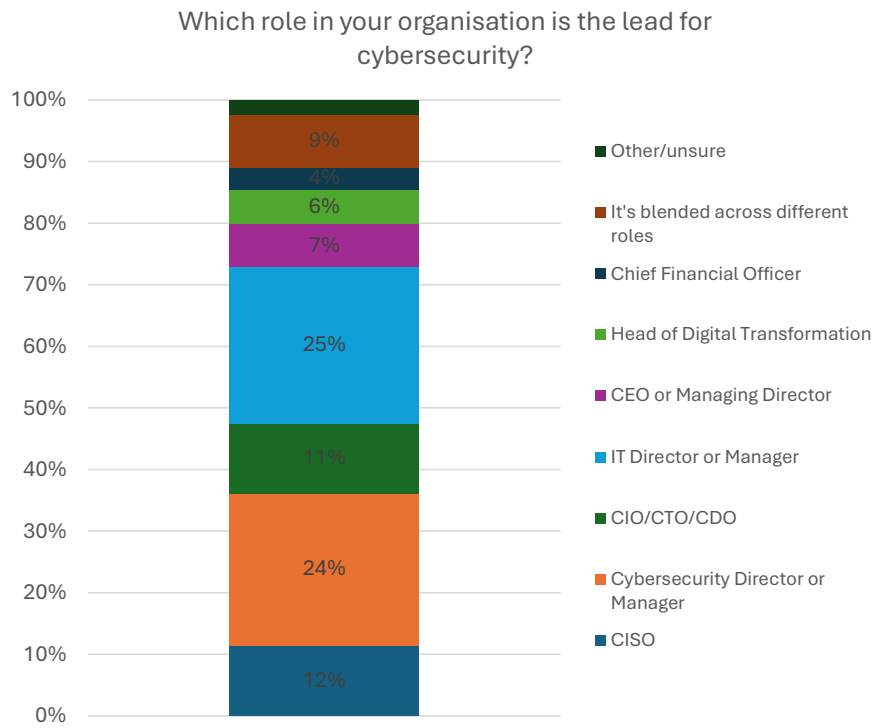
Understanding the structure, responsibilities and reporting lines can accelerate commercial engagement, however the data suggests it's not a uniform environment:

- 39% of companies have a dedicated cybersecurity team that operates from within the IT department
- 36% have a dedicated cybersecurity team that operates independently, outside of the IT department
- 18% have IT staff that assume cybersecurity responsibilities in addition to the full-time IT role for which they were hired
- 5% outsource 100% of their cybersecurity operations to partners.

Who holds responsibility?

Well, it's a bit of a mixed bag and cybersecurity leadership varies across markets. However, the most common leader is the IT manager or director in 25% of companies, followed by:

1. Cybersecurity directors/managers – 24%
2. CISOs – 12%Zxc
3. CIOs/CTOs/CDOs – 11%



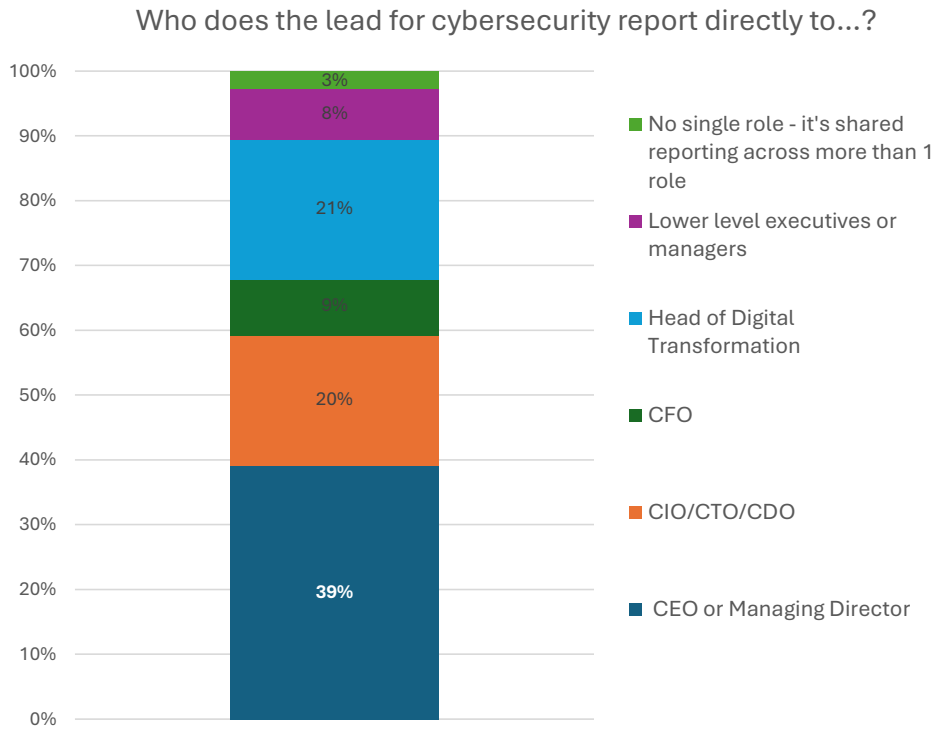
SOPHOS

Navigating cybersecurity structures

Who has ultimate oversight of cybersecurity operations? Unsurprisingly our data shows the CEO or MD takes top spot, with 39% of companies stating the cybersecurity leader reports directly to this role.

Double-clicking on the data also shows those reporting to CEOs and MDs are typically CIOs/CTOs/CDOs as well as CISOs.

Interestingly, Digital Transformation Leaders take second spot, with 21% of companies saying they hold executive oversight, closely followed by CIOs/CTOs/CDOs at 20%.



Key Partner Takeway
80% of executive oversight for cybersecurity is held by 3 key roles and messaging to each is nuanced and different.

- *For CEO/Managing Directors lead with guidance on risk exposure, disruption of business operations (aka 'cyber resiliency') and compliance.*
- *For CFOs lead with an emphasis on cyber resiliency, cost optimisation and value realisation, and risk exposure and mitigation.*
- *For CIOs/CTOs/CDOs lead with augmentation of skills and technologies (especially automation and artificial intelligence), platform and integration capabilities, and cybersecurity education to the board, executive team and wider business.*

SOPHOS

TRA

Regulatory and legislative change is good for MSPs (yes, really)

The impact of tighter regulatory and legal frameworks on cybersecurity professionals, boards and executive management teams is being felt extensively.

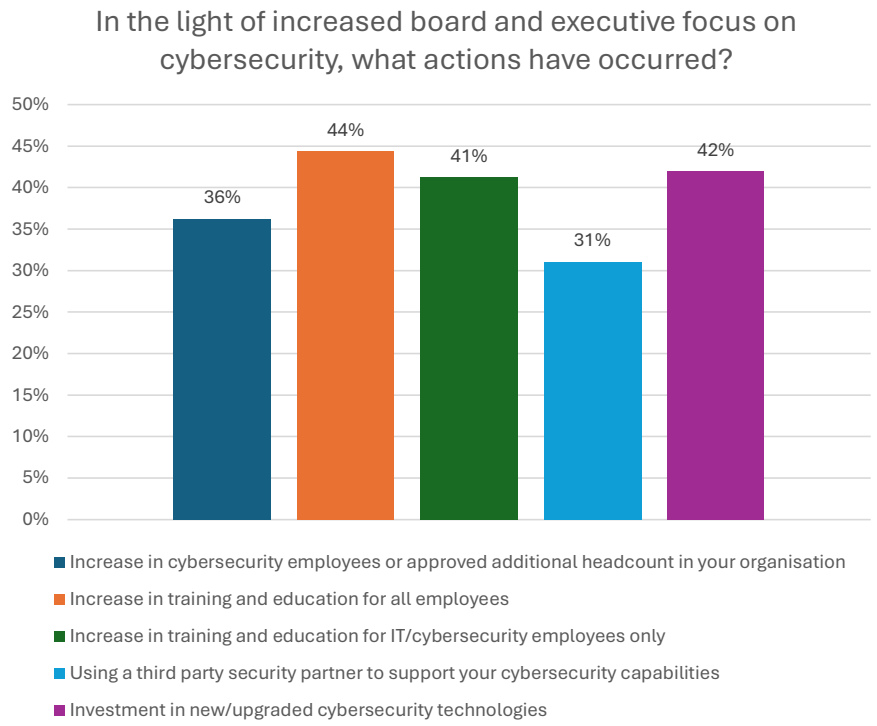
95% of Asia Pacific businesses state that legislation and regulatory changes mandating cybersecurity responsibilities and liabilities have increased the focus on cybersecurity at a board and leadership team level.

44% say this has increased 'a lot' and a further 51% say it is increased by a 'little'.

This is good news for MSPs as businesses have boosted cybersecurity focus in a number of areas including:

- 44% increasing employee education & training,
- 42% investing in new/upgraded cybersecurity technologies,
- 41% increasing IT/cybersecurity employee education % training, and
- 31% increasing usage of MSPs in more areas.

Key Partner Takeaway
Demonstrating a clear appreciation of government cybersecurity programmes, legislative, data protection and personally identifiable information (PII) requirements, and data breach and disclosure laws (in place or planned) is critical when engaging at senior levels of organisations.



SOPHOS

TRA

Engaging Boards and Executive Teams

Regulatory and legal changes are having an impact and this has created opportunities for MSPs to deeper engagement with boards and executive teams.

Our data highlights only 51% of boards and 54% of executive management teams are considered to 'truly' understand' cybersecurity issues by their own IT and cybersecurity professionals.

The data shows for companies with boards or executive teams that don't truly understand cybersecurity there are a number of concerns including being in breach of statutory requirements, increased risk exposure and a lack of investment in cybersecurity.

However another key implication stood out –repeat offenders.

38% of companies stated board members make ongoing mistakes despite participating in cybersecurity education and training programmes.

The number jumped to 41% for executive teams, with the data showing moderate correlation between board lapses and executive team lapses.

Key Partner Takeway
Ensuring clear messaging on key topics for boards and executive teams is critical consideration, and reducing repeat offender rates has a positive upside on investment in cybersecurity solutions and capabilities.

Key Board and Executive Team Topics of Interest		
Rank	**Board**	**Executive Team**
1	Board obligations and requirements	Developing a cybersecurity strategy
2	Creating an incident response plan	Understanding the evolving threat landscape
3	Identifying and understanding relevant legislation	Supporting cybersecurity burnout and fatigue
4	Identifying and prioritising security focus – crown jewels, baubles and trinkets	Practical steps to take in the event of a breach
5	Identifying and assessing cybersecurity gaps	Identifying and prioritising security focus – crown jewels, baubles and trinkets

SOPHOS

TRA

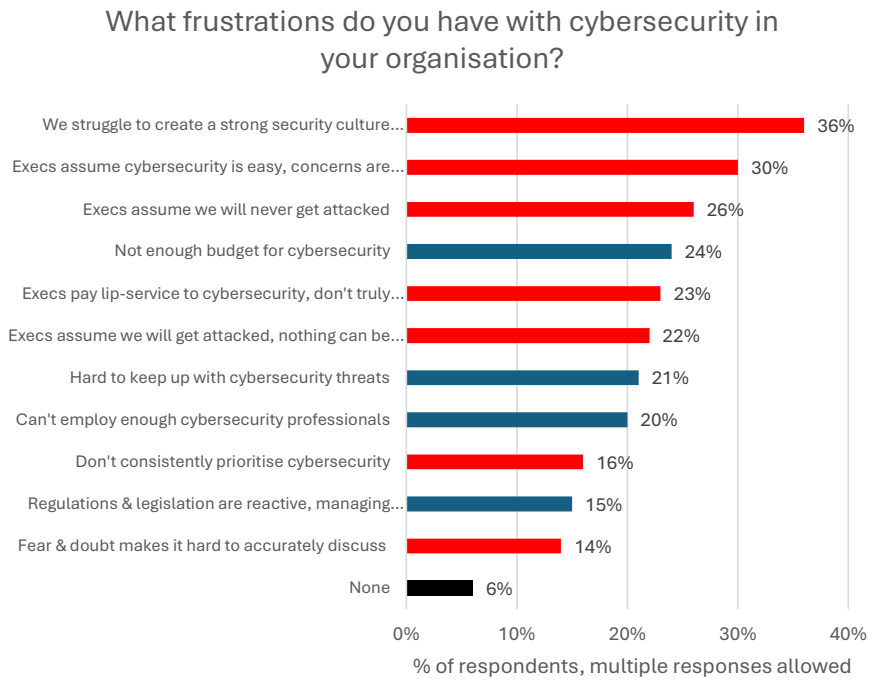
Cybersecurity Key Strategic Pain Points

Do you think technology is the key pain point for many organisations' cybersecurity operations? Think again.

We asked cybers7ecurity professionals about key pain points and frustrations experienced with cybersecurity inside their organisations. Cultural issues feature significantly and are areas of opportunity for MSPs to engage with businesses.

Creating and maintaining a strong security culture across the entire company is cited as the most significant frustration. A misfiring culture is also intertwined with executive postures and preconceived notions about cybersecurity importance, effectiveness and breach inevitability.

Operational issues focus on lack of budgets available to support cybersecurity goals, the speed of the evolving threat landscape, lack of skilled inhouse resources, and an increasingly complex and changing regulatory and legal requirements.



Key partner takeaway
Partners have strong opportunities to support customers instilling cybersecurity cultures and beliefs, as well as being a logical solution to budget constraints, lack of skilled inhouse resources, keeping abreast of threats and regulatory landscapes.

Legend: Culture Operations

SOPHOS

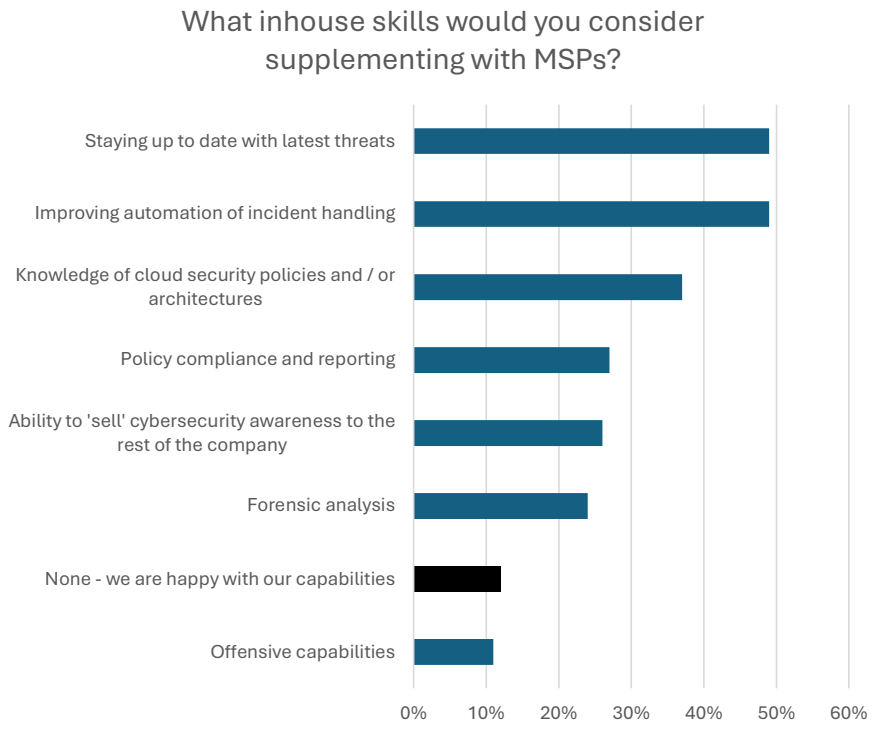
Solving the Customer Skills Shortage

Very few organisations (12%) don't use MSPs to augment their internal cybersecurity skills.

There's clear demand for partners to bring a mixture of skills to support businesses including:

- Professional advisory services (such as keeping up to date with evolving threat landscapes and compliance requirements),
- Technology (automation, cloud security policies, compliance and architecture, forensic analysis and offensive capabilities), and
- Educating and creating strong awareness of cybersecurity amongst the broader organisation.

Key Partner Takeaway: Building on the cultural and operational issues mentioned in previous pages, having a blended offer that incorporates practical professional services and technology skills is an important consideration for many businesses.



SOPHOS

TRA

Cybersecurity burnout and fatigue: The ‘hidden’ symptom undermining effective operations

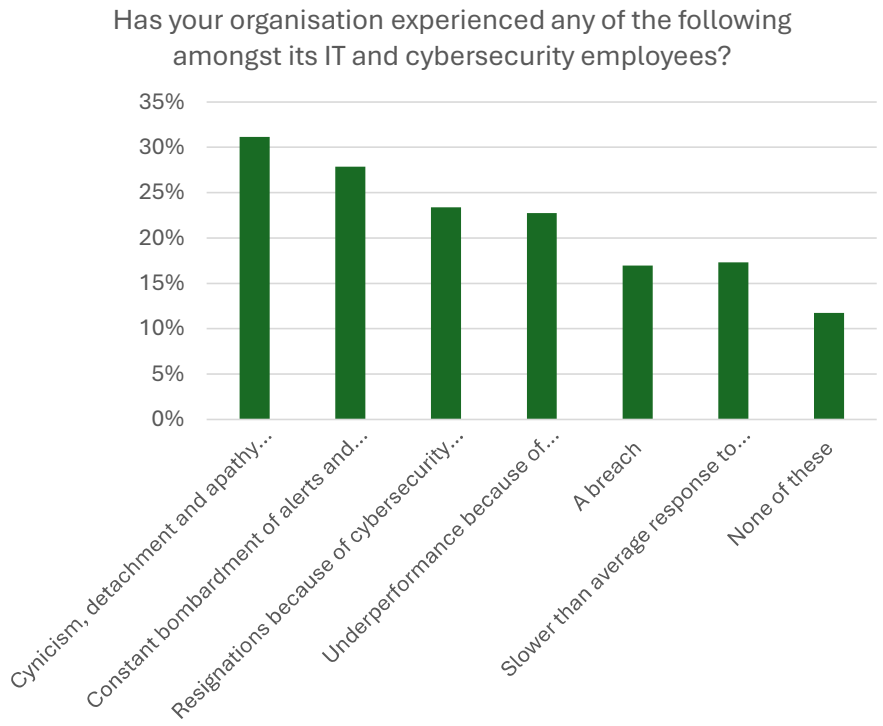
Our “*4th edition of the “The Future of Cybersecurity in Asia Pacific and Japan*” authored for Sophos revealed cybersecurity burnout and fatigue are critical issues that weaken cybersecurity operations and effectiveness:

- 85% of companies stated they experience fatigue and burnout among their cybersecurity and IT professionals, almost 1-in-4 (23%) experience this issue ‘frequently’, and 62% ‘occasionally’.
- 90% of companies state burnout and fatigue have increased in the last 12 months, 30% of these saying the increases have risen ‘significantly’ .

The impacts are considerable on both employees and business operations.

Employees stated:

- 41% felt they are not diligent enough in their performance,
- 34% felt heightened levels of anxiety if subject to a breach or attack,
- 31% experience feelings of cynicism, detachment and apathy towards their responsibilities
- 30% stated it makes them want to either resign or change career, and
- 23% have resigned due to cybersecurity burnout and fatigue.



SOPHOS

TRA

Cybersecurity burnout and fatigue: The business impact

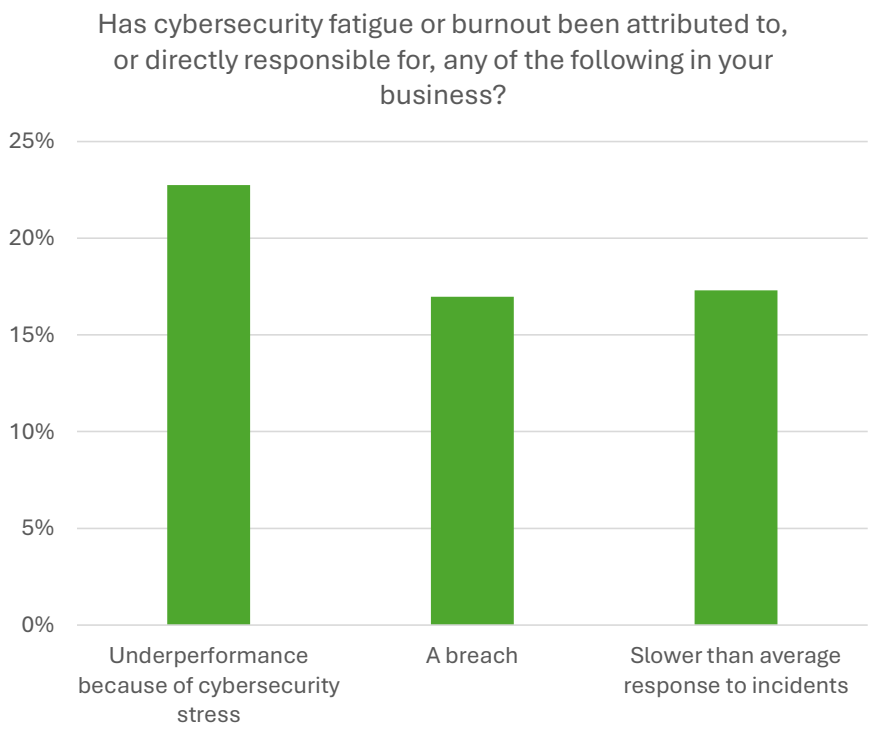
There are a number of ways cybersecurity burnout and fatigue directly impacts on businesses, and where MSPs can offer support:

- Lost productivity: Burnout and fatigue is responsible for an average productivity loss of 4 .1 hours per week amongst cybersecurity and IT professionals.
- Direct contribution to breaches: 17% of organisations identified that cybersecurity burnout or fatigue contributed to, or was directly responsible for, a cybersecurity breach .
- Resignations and 'moving employees on': Stress and burnout were directly attributed as a cause of cybersecurity and IT professional resignations in 23% of companies .

The most common causes include:

1. Not having the inhouse resources (budgets, people, technology) to support cybersecurity activities,
2. The routine aspects of the role creating monotony, interspersed with challenging activity,
3. Increased board and/or executive management pressure due to regulatory and legal obligations,
4. Alert overload requiring prioritisation, even if the majority are false alarms
5. Increased threat activities and adoption of new technologies (e.g., AI).

Key Partner Takeaway
Whilst potentially an uncomfortable topic for some, the prevalence of fatigue and burnout has a detrimental impact on many organisations. Raising the topic can provide an effective segue into the role partners can play in helping organisations address the impacts on employee and business performance.



SOPHOS

TRA

Partners are critical to cybersecurity delivery and support, and doing a pretty good job

Reflecting the hard work dedicated to learning about, and aligning with customers, the data shows strong synchronisation between what MSPs think customers want from them, and what customers told us they look for in prospective MSPs.

Business use of MSPs is high, satisfaction is strong and future intent to engage is positive:

- 68% of businesses use at least 1 MSP today, with 50% of these using multiple partners to support their cybersecurity activities,
- Another 28% of companies plan to use MSPs in the future, and
- Satisfaction with partners is strong, at an average rating of 7.5 out of 10.

Key Partner Takeaway
The top 7 customer 'MSP wants' are relatively strategic and holistic in nature, the next 7 are operationally focused with a product emphasis – security operations (patching, firewalls, antivirus, etc), XDR/MDR solutions, incident response and remediation, threat hunting, PII protection and penetration testing.

Customer MSP 'Wants' vs MSPs' Understanding

Rank	What customers want from MSPs	What MSPs think customers want from them
1	Depth of knowledge – landscape, threats, recovery	Depth of knowledge – landscape, threats, recovery
2	Competitive costs and value realisation	Competitive costs and value realisation
3	Cybersecurity as a Service	Cybersecurity as a Service
4	Regulatory, legislative and compliance knowledge	Cybersecurity innovation
5	Cybersecurity innovation	Regulatory, legislative and compliance knowledge
6	AI solutions to incorporate into cybersecurity	AI solutions to incorporate into cybersecurity
7	Quicker access to vendors' new products & solutions	Quicker access to vendors' new products & solutions

SOPHOS

TRA

Common mistakes MSPs make selling to businesses

So, it's a competitive market, MSPs are in demand and you're looking to win new business.

Want to know the common mistakes your competitive peers make? Read on.

Our analysis suggests we can determine 2 main points of failure:

- Failing to be considered by the customer by not overcoming common generic concerns about using third party MSPs, and
- Making the consideration stage yet failing to clearly articulate the MSP value.

Key Partner Takeaway
These mistakes are not technology related, rather they point to underperforming market positioning, sales engagement and message articulation. Work with vendor partners to tailor responses to overcome common objections to MSPs and ensure a focus on business values and outcomes that is underpinned by competitive pricing and product excellence. If your vendor won't help, find one that will.

Common Selling Mistakes made by MSPs

Rank	Top concerns about using 3rd party MSPs	Top MSP sales mistakes
1	"I'll lose control."	"They just didn't understand our business problem."
2	I'm not sure I trust you with access to our data, systems and IP."	"Their account and communication skills were terrible, I didn't trust them to run our cyber operations."
3	"You promise quality but deliver poor service."	"All they did was try and push products at me."
4	"I won't have true visibility into costs and value."	"Selling at me without strong business case and value realisation metrics won't work."
5	"Our data is too sensitive to let someone else protect it."	"The pricing was just uneconomical, contract terms were inflexible."
6	"The minute I want flexibility, I'll have to pay for scope changes."	"I'll buy when I want to, not because it's your month or quarter end."
7	"I won't have visibility into your cybersecurity operations so how do I know I'm secure?"	"You didn't engage our procurement team and tried to bypass them? Hah, good luck."

SOPHOS

TRA

Country Data: Australia

Partner Engagement

% currently using MSPs: 68%

% planning to engage in future: 24%

Satisfaction level: 7.4 / 10

#1 Reason companies don't want to work with MSPs: Loss of control

Top MSP selling mistake: Not understanding the business problem

Top cybersecurity frustration experienced by businesses

"We struggle to create and maintain a strong cybersecurity culture across the whole company."

Board and executive team topics of interest

Board: How to create an incident response plan

Executive team: Prioritisation – identifying crown jewels, baubles and trinkets

Cybersecurity and burnout

Productivity lost: 3.8 hours per week

Contribution to breaches: 19%

Cybersecurity structure

- 43% have dedicated cybersecurity team working within the IT group
- 37% have dedicated cybersecurity team working outside of the IT group

Cybersecurity Responsibility

- 28% IT Manager or Director
- 21% CISO

Executive Responsibility

- 51% CEO or Managing Director
- 22% CIO/CTO/CDO

SOPHOS

TRA

Country Data: India

Partner Engagement

% currently using MSPs: 75%

% planning to engage in future: 25%

Satisfaction level: 8.2 / 10

#1 Reason companies don't want to work with MSPs: Not trusting a 3rd party with access to data and systems.

Top cybersecurity frustration experienced by businesses

"Our executives assume cybersecurity is easy and our concerns are over exaggerated."

Board and executive team topics of interest

Board: How to create an incident response plan

Executive team: The evolution of AI and ML in the cybersecurity space

Cybersecurity and burnout

Productivity lost: 3.6 hours per week

Contribution to breaches: 22%

Cybersecurity structure

- 36% have dedicated cybersecurity team working within the IT group
- 42% have dedicated cybersecurity team working outside of the IT group

Cybersecurity Responsibility

- 29% IT Manager or Director
- 7% CISO

Executive Responsibility

- 41% CEO or Managing Director
- 21% CIO/CTO/CDO

Country Data: Japan

Partner Engagement

% currently using MSPs: 60%

% planning to engage in future: 33%

Satisfaction level: 6.7 / 10

#1 Reason companies don't want to work with MSPs: Not trusting a 3rd party with access to data and systems.

Top cybersecurity frustration experienced by businesses

"The executive team pay lip service to cybersecurity but don't truly believe in it."

Board and executive team topics of interest

Board: How to create an incident response plan

Executive team: The evolution of AI and ML in the cybersecurity space.

Cybersecurity and burnout

Productivity lost: 3.6 hours per week

Contribution to breaches: 5%

Cybersecurity structure

- 36% have dedicated cybersecurity team working within the IT group
- 26% have dedicated cybersecurity team working outside of the IT group

Cybersecurity Responsibility

- 12% IT Manager or Director
- 13% CISO

Executive Responsibility

- 23% CEO or Managing Director
- 22% CIO/CTO/CDO

Country Data: Malaysia

Partner Engagement

% currently using MSPs: 74%

% planning to engage in future: 25%

Satisfaction level: 7.9 / 10

#1 Reason companies don't want to work with MSPs: Potential loss of control.

Top cybersecurity frustration experienced by businesses

"We struggle to create and maintain a strong cybersecurity culture across the whole company."

Board and executive team topics of interest

Board: Obligation and role of the board, directors and the executive team in cybersecurity.

Executive team: The impact of cybersecurity burnout amongst employees.

Cybersecurity and burnout

Productivity lost: 4.1 hours per week

Contribution to breaches: 21%

Cybersecurity structure

- 41% have dedicated cybersecurity team working within the IT group
- 40% have dedicated cybersecurity team working outside of the IT group

Cybersecurity Responsibility

- 21% IT Manager or Director
- 13% CISO

Executive Responsibility

- 42% CEO or Managing Director
- 14% CIO/CTO/CDO

Country Data: Philippines

Partner Engagement

% currently using MSPs: 63%

% planning to engage in future: 29%

Satisfaction level: 8.0 / 10

#1 Reason companies don't want to work with MSPs: Potential loss of control.

Top cybersecurity frustration experienced by businesses

Equally shared between "Our executives assume we will never get attacked." and "Our executives assume cybersecurity is easy and our concerns are over exaggerated."

Board and executive team topics of interest

Board: Obligation and role of the board, directors and the executive team in cybersecurity.

Executive team: The evolution of AI and ML in the cybersecurity space.

Cybersecurity and burnout

Productivity lost: 4.6 hours per week

Contribution to breaches: 11%

Cybersecurity structure

- 37% have dedicated cybersecurity team working within the IT group
- 40% have dedicated cybersecurity team working outside of the IT group

Cybersecurity Responsibility

- 31% IT Manager or Director
- 8% CISO

Executive Responsibility

- 45% CEO or Managing Director
- 14% CIO/CTO/CDO

Country Data: Singapore

Partner Engagement

% currently using MSPs: 69%

% planning to engage in future: 28%

Satisfaction level: 7.4 / 10

#1 Reason companies don't want to work with MSPs: Costs.

Top cybersecurity frustration experienced by businesses

"We struggle to create and maintain a strong cybersecurity culture across the whole company."

Board and executive team topics of interest

Board: Obligation and role of the board, directors and the executive team in cybersecurity.

Executive team: Practical steps to take in the event of a breach.

Cybersecurity and burnout

Productivity lost: 4.2 hours per week

Contribution to breaches: 23%

Cybersecurity structure

- 41% have dedicated cybersecurity team working within the IT group
- 33% have dedicated cybersecurity team working outside of the IT group

Cybersecurity Responsibility

- 36% IT Manager or Director
- 5% CISO

Executive Responsibility

- 35% CEO or Managing Director
- 24% CIO/CTO/CDO

About

Data referenced in this report is drawn from TRA's research for Sophos conducted in January 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

SOPHOS

TRA