SOPHOS

The Future of Cybersecurity in Asia Pacific and Japan

4th Edition, February 2024

A TRA Report sponsored by Sophos

This report focuses on cybersecurity burnout and fatigue and the impact they have on employees and the organisations in which they work in the Asia Pacific and Japan

Contents

Introduction

Welcome to the 4th edition of the "The Future of Cybersecurity in Asia Pacific and Japan".

First published in 2019, the reports have examined cybersecurity issues confronting businesses throughout Australia, India, Japan, Malaysia, The Philippines and Singapore.

Previous editions focused on areas including cybersecurity maturity, board level understanding of cybersecurity, common inhibitors limiting the success of cybersecurity programmes and other practical factors shaping how companies manage their cybersecurity environment.

This edition is different.

It focuses primarily on cybersecurity burnout and fatigue and their impact on employees and the organisations in which they work.

Our research reveals the frequency of attacks, alert fatigue, internal struggles with education and training and, increasingly, the growing demands of boards and senior management teams, are degrading cybersecurity and IT professionals' abilities to maintain a strong security posture.

Burnout is felt across almost all aspects of cybersecurity operations and has increased: 30% of organisations say that feelings of burnout have increased 'significantly' in the last 12 months and 41% of professionals say that it makes them 'less diligent' in their cybersecurity roles.

Other key findings include:

- 75% of companies have a dedicated cybersecurity team and 5% of companies fully outsource their cybersecurity operations to third party firms.
- IT and cybersecurity professionals feel 49% of boards and 46% of senior leadership teams (SLTs) do not fully understand cybersecurity.
- ...yet 95% of these groups have increased their focus on cybersecurity as a result of increased regulatory and other legal requirements.
- 6-in-10 boards, and 1-in-2 SLTs do not regularly receive cybersecurity updates.
- 81% of cybersecurity and IT professionals have experienced their personal data being lost as a customer of another company.
- This personal data loss has direct implications for the organisation in which they currently work including heightened concerns, stress and the inevitability of a data breach.
- 41% of SLTs, 38% of employees and 28% of boards contain repeat offenders that continue to make common cybersecurity mistakes despite ongoing training and education campaigns.
- 84% of companies have incident response and breach communications plans in place yet their effectiveness is questionable: 29% of companies say their response is 'chaotic' when attacked or breached and 26% say they perform professionally and do a good job.
- 75% of those plans were developed after a breach or attack.

For details about the data survey please refer to "Survey Demographics and Methodology" in the Appendix.

The Research Findings

The research results are presented in five sections:

1. Cybersecurity burnout
2. Boards, C-Suites and Cybersecurity
3. The cybersecurity setup
4. Incident response and recovery
5. Cybersecurity and IT professionals' areas of concern and frustration

Cybersecurity burnout

Prevalence of Burnout

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'.

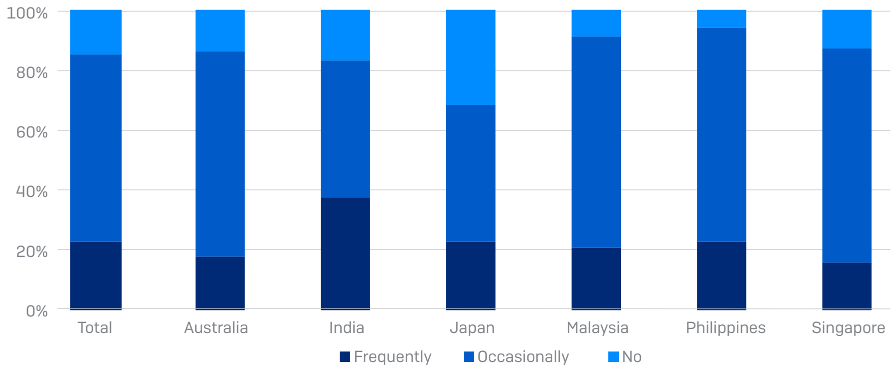
A lower level of burnout and fatigue in Japan (69%) decreases the average across our survey countries. Excluding the Japanese data, burnout levels are high (greater than 80% of all organisations) in Australia, India, Malaysia, The Philippines and Singapore.

37% of Indian organisations state feelings of burnout and fatigue are 'frequently' experienced (significantly higher than the 23% average) and more than 90% of companies in The Philippines (94%) and Malaysia (91%) are impacted by burnout and fatigue.

The prevalence of burnout and fatigue is not dropping. Troublingly, 90% of companies state burnout and fatigue have increased in the last 12 months, 30% of these saying the increases have risen 'significantly'.

Indian (48%) and Japanese (38%) companies show the highest rates of 'significant' growth in burnout and fatigue in the past 12 months, whilst firms in The Philippines (21%) and Singapore (18%) indicate lower than average levels of 'significant' growth.

Have you, or one of your cybersecurity or IT colleagues experienced feelings of cybersecurity fatigue or burnout?



The Impact of Cybersecurity Burnout and Fatigue

The impact is felt on both employees and employers. To understand how it manifests in both groups, our survey cohort included responses from both cybersecurity and IT employees as well as those in cyber management or oversight roles.

Let's start with employees.

Cybersecurity burnout and fatigue impact on employees

Across Asia Pacific, approximately 90% of all cybersecurity and IT employees are negatively impacted by burnout and fatigue. Just 10% of employees stated they did not feel any impact on their work performance.

90% is a troubling statistic.

At a time when organisations are struggling with cybersecurity skills shortages and an increasingly complex threat environment, employee stability and performance are of paramount importance. Burnout and fatigue are undermining both areas, and our data revealed that, on average:

- 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 cybersecurity activities and their responsibilities
- 30% stated it makes them want to either resign or change career (23% of all surveyed have acted on this and resigned)
- 10% feel guilty that they cannot do more in their role to support cybersecurity activities

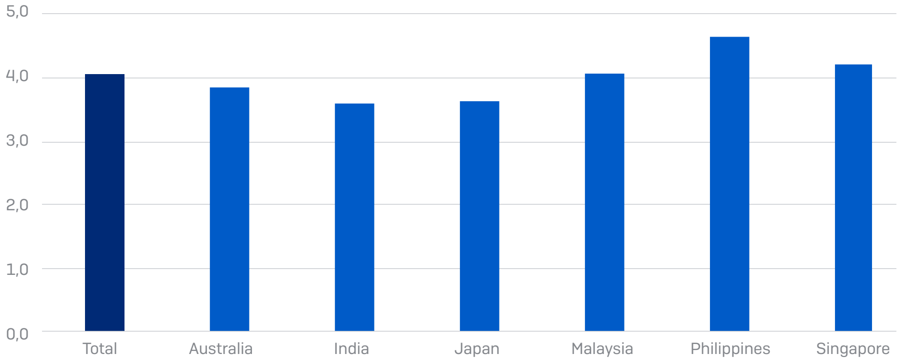
Guilt, apathy, detachment and anxiety. No wonder employees are struggling, and businesses are impacted.

Cybersecurity burnout and fatigue impact on business operations

There are 4 key areas where cyber burnout and fatigue has direct impact on business operations:

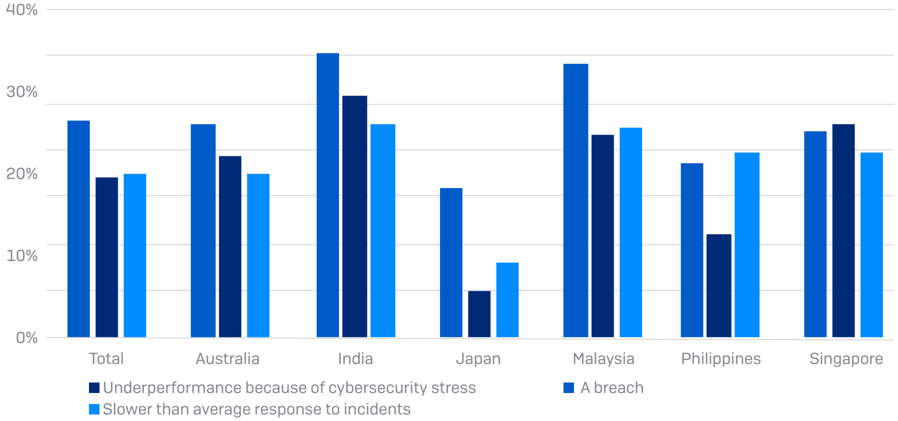
1. Lost productivity: On average, businesses are experiencing a productivity loss of 4.1 hours per week amongst cybersecurity and IT professionals due to burnout and fatigue. Companies in The Philippines (4.6 hours/week) and Singapore (4.2 hours/week) were the worst impacted while India and Japan (both 3.6 hours/week) were the least affected.

Have you or members of the IT/cybersecurity team have lost productivity due to cybersecurity fatigue? If yes, please tell us how many hours per week lost. (Average)



2. Direct contribution to breaches: On average, 17% of organisations identified that cybersecurity burnout or fatigue contributed to, or was directly responsible for, a cybersecurity breach. India (25%), Singapore (23%), Malaysia (21%) and Australia (19%) revealed rates higher than the average, while Japan (5%) and The Philippines (11%) were lower.

Has cybersecurity fatigue or burnout been attributed to, or directly responsible for, any of the following?

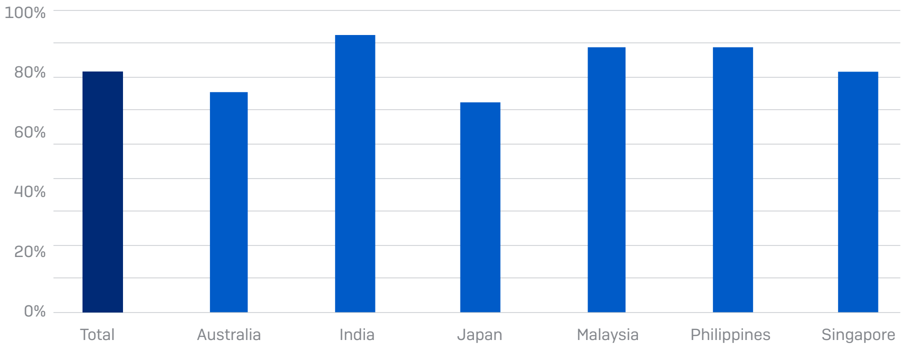


Slower response times to cybersecurity incidents: 17% of companies experienced slower than average response times. Companies in India and Malaysia suffered from the highest proportion with slower response times (both at 22%), followed by Singapore (20%), The Philippines (19%) and Australia (17%). Japanese data was significantly lower than the average at 8%.

3. Resignations and 'moving employees on': Stress and burnout were directly attributed as a cause of cybersecurity and IT professional resignations in 23% of companies. However, that number masks considerable variations across countries: for example, Singapore (attributed to 38% of resignations) and India (31%) are considerably higher. Organisations also noted that, on average, 11% of them had 'moved on' a cybersecurity or IT employee as result of the individual being impacted by stress or burnout. Malaysia (28% of companies) and Singapore (15%) had the highest incidence of this practice.

Businesses appear cognizant of the need to provide support to employees facing cybersecurity burnout and fatigue, with 71% across the region providing stress counselling support to IT and cybersecurity professionals.

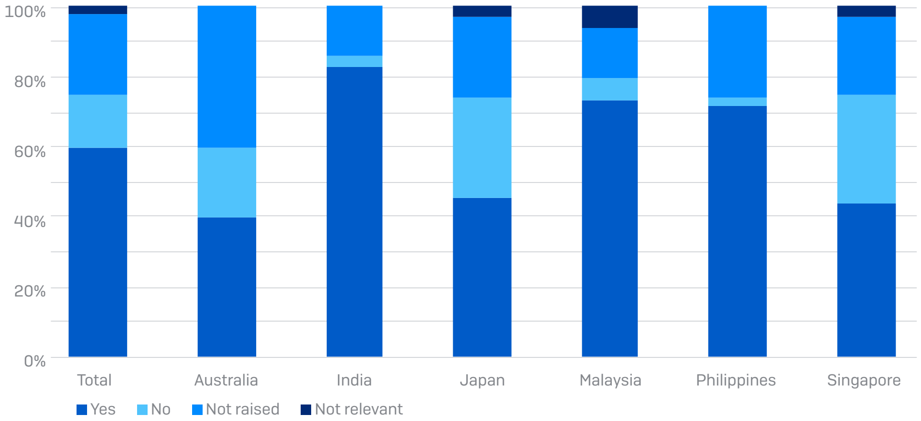
Does your organisation provide cybersecurity stress counselling for IT/cybersecurity employees? "Yes"



There is growing acceptance of the importance of discussing mental health and related issues in a work context. It is pleasing to see that employees in some countries received a positive response from their organisation once they raised concerns with fatigue and burnout.

Employees in India (83% stated positive response), Malaysia (74%) and The Philippines (71%) all noted positive responses above the overall average (60%) whilst Australia (40%), Singapore (44%) and Japan (46%) were below average.

If you have raised concerns about cybersecurity fatigue with your organisation, did you receive a positive response?

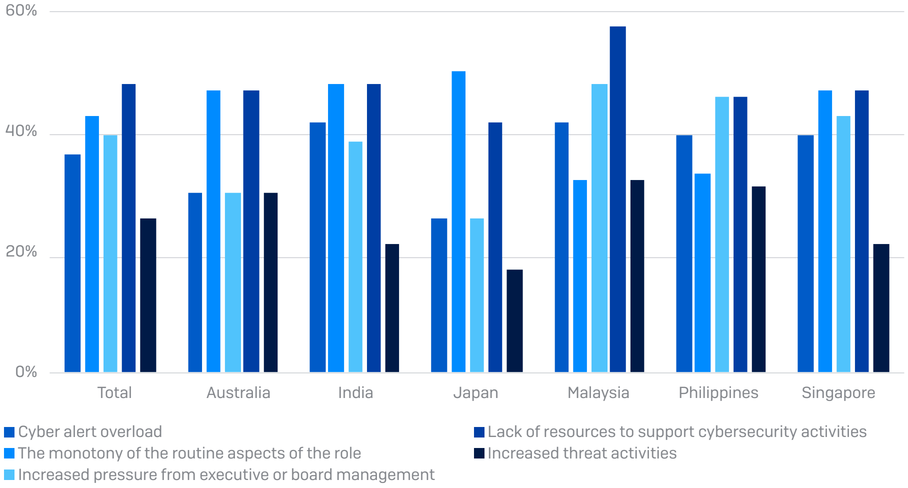


Causes of cyber burnout and fatigue

The top 5 main causes are a mixture of the role, resources shortages and management pressure, namely:

1. Lack of resources available to support cybersecurity activities including staff shortages, budget restrictions and limited third party support
2. The routine aspects of the role create a feeling of monotony, interspersed with challenging moments of activity
3. An increased level of pressure from board and/or executive management, increasingly as these groups come under pressure from changing regulatory and legal obligations relating to cybersecurity
4. Alert overload where professionals are faced with persistent alerts from tools and systems, all of which require prioritisation and action, even if the majority are false alarms
5. The increase in threat activity and the adoption of new technologies that have contributed to a more challenging, 'always on' environment

Top 5 Causes of Cyber Burnout and Fatigue



Given the importance of boards and executive leadership teams in driving company, technology and cybersecurity strategies, it is important to note that increased pressure from these groups is contributing to cybersecurity burnout and fatigue.

Let's take a look at board and C-suite levels of cybersecurity understanding, how this has changed from previous reports and what impact regulatory and legislative changes are having on cybersecurity at these levels.

Boards, C-Suites and cybersecurity

In our 3rd edition, we noted "Approximately only 4 in 10 cybersecurity professionals believe their company board truly understands cybersecurity."

Pleasingly the data shows an increase in this year's data to 51%, suggesting improved levels of understanding.

In previous editions we had not incorporated data from the senior leadership team (SLT) alongside board level data however it has been included this year.

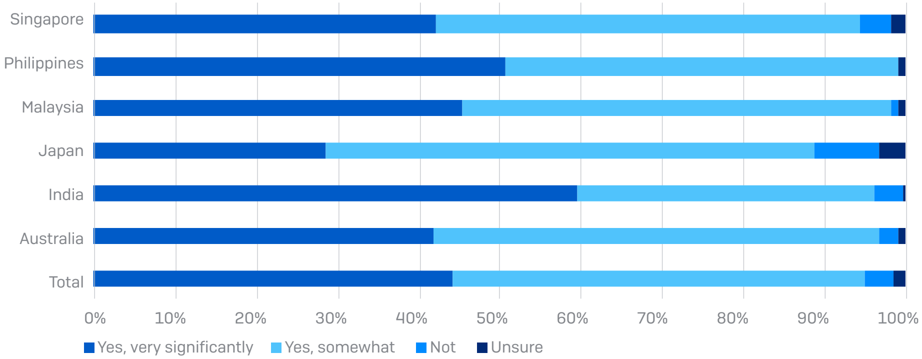
We found the SLT data shows marginally higher levels of understanding (54%) compared to the board (51%). In part this can be attributed to the rise in prominence of cybersecurity as part of top 10 business priorities (currently sitting in 2nd place, having risen steadily from 9th place 5 years ago) however there is another factor at play here: mandated responsibility.

Many countries in Asia Pacific and Japan have introduced, or are introducing, legislation that requires organisations to disclose cybersecurity breaches, and while we're not legal eagles, the view amongst our learned friends in the legal profession is that board and SLT duty of care requirements will ultimately be extended to cybersecurity breaches for boards and SLT executives.

In other words, a breach may ultimately be considered as part of the areas boards and SLT are duty bound to ensure they are doing all within their power to manage and protect.

Our data reflects the impact that these regulatory changes are already bringing to boards, SLTs and cybersecurity: On average, 44% of respondents stated that mandated responsibilities had increased the focus on cybersecurity 'very significantly' and another 51% felt that it contributed 'somewhat'.

Have legislation and regulatory changes mandating cybersecurity board level responsibilities and liabilities increased the focus on cybersecurity at a company board or director level?



So, boards and SLTs are under increasing pressure to manage company cybersecurity environments. One in two SLTs don't understand cybersecurity, and employees are stating they are feeling the heat from management to meet cybersecurity performance expectations. This could end badly.

Without appropriate support, burnout and fatigue rates will only increase.

On a positive note, as organisations begin to appreciate the issues faced, support seems to be moving in the right direction. Our data shows five key areas that are benefiting:

1. 44% of our sample indicated they are increasing funding for cybersecurity education and training across all employees in their organisations
2. 42% are also increasing funding for new/upgraded cybersecurity technology solutions
3. 41% are investing in education and training specifically for their cybersecurity and IT employees
4. 36% are lifting cybersecurity headcount through new hires
5. 31% are increasing their investment in third party cybersecurity partners

In short, cybersecurity burnout and fatigue is a critical issue impacting organisations and employees on multiple levels. As attack frequencies increase, along with deployment of new technologies (by both companies and threat actors) and heightened executive management expectations and focus, many organisations risk seeing a degradation of their cybersecurity capabilities, exposing their operations to potentially crippling circumstances.

With this in mind, we turn our attention to some of the other practical issues around cybersecurity that we've analysed in previous editions.

We'll start with what we term the 'cybersecurity setup', i.e, the structure of cybersecurity in companies and which roles hold responsibility.

The cybersecurity setup: responsibilities, reporting lines and reporting frequency

Leadership for cybersecurity is highly varied across and within all markets. However, the most common leader is the IT manager or director (between 36% in Singapore and 21% in Malaysia). In Malaysia (21%), Philippines (33%) and Japan (28%) a Cybersecurity director is also a common leader. Australia has 21% nominating a CISO.

Interestingly, 9% of organisations state that leadership is shared across multiple roles rather than a single cybersecurity designated leader. This approach was highest in Malaysia (13%) and Singapore (11%) and lowest amongst Indian organisations (5%).

39% say the cybersecurity leader reports directly to the CEO; it is highest in Australia with 51% and lowest in Japan (23%) where 26% say cybersecurity leaders report to the Head of Digital Transformation. The third most common reporting line is to the CIO/CTO.

75% of companies have a dedicated cybersecurity team, with 39% saying this sits within the IT department. Japan has the highest percentage (25%) of organisations where IT staff are also tasked with cybersecurity responsibilities. Across the region, 5% say they have their cybersecurity 100% outsourced (8% in Japan and 7% in Singapore).

A new area of focus this year is the frequency of briefings cybersecurity leaders provide to internal stakeholders and external groups such as customers, partners and government agencies.

We'd respectfully submit that despite increased focus on cybersecurity amongst boards and SLTs, there is more work to be done on providing updates to key stakeholders:

- On average only 41% of boards and 51% of SLTs are provided with regular updates on cybersecurity
- Within this dataset, the frequency of updates is positive, with 37% of boards and 27% of SLTs receiving weekly updates and a further 36% of boards and 39% of SLTs receive monthly updates
- 6 in 10 boards and one in two SLTs are not receiving regular cybersecurity updates

	Total	Australia	India	Japan	Malaysia	Philippines	Singapore
The board	41%	49%	46%	21%	49%	52%	38%
The executive committee	51%	46%	53%	38%	65%	60%	58%
Company-wide	45%	47%	48%	36%	56%	41%	51%
3rd party vendors and suppliers	22%	21%	27%	13%	29%	25%	25%
Government officials	19%	18%	26%	4%	33%	11%	29%
Customers	16%	12%	21%	12%	20%	13%	24%
Informal updates only	2%	1%	0%	5%	1%	4%	3%
No	1%	1%	0%	1%	0%	1%	0%

Table 1 "Q: Are regular cybersecurity updates and briefings provided by your company to any of the following groups?"

Incident response and recovery

Rather than provide data this year on breach rates (we'll come back to that next edition), we wanted to examine factors related to incident response and recovery, namely:

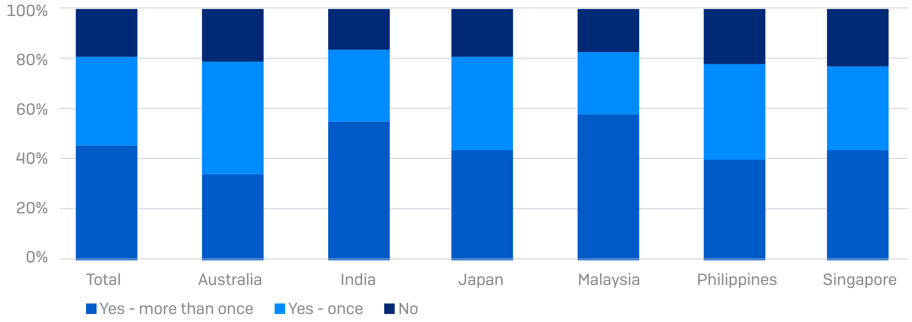
- The impact of cybersecurity and IT employees personally experiencing a breach outside of their employer and how it impacts their view of their own company's cybersecurity activity
- How many organisations have formal incident response plans in place and the driver to develop those plans
- Do repeat offenders of cybersecurity lapses learn from their mistakes?
- How organisations self-rate their own cybersecurity incident response readiness

The impact of a personal breach

We were curious to understand how a personal cyber breach[1] experienced by a cyber-security or IT professional impacts their view of their own organisation's cybersecurity.

In what is probably a very relatable statistic to many readers, 81% of respondents have already experienced a personal cyber breach. Unlike other variations across our data set in other questions, the differences for individual countries are relatively minor, suggesting a degree of uniformity across all countries.

As an individual in your personal life, outside of your company, have you experienced, or been notified, about your own personal details being lost or compromised in a security breach? (Rounding may effect totals)



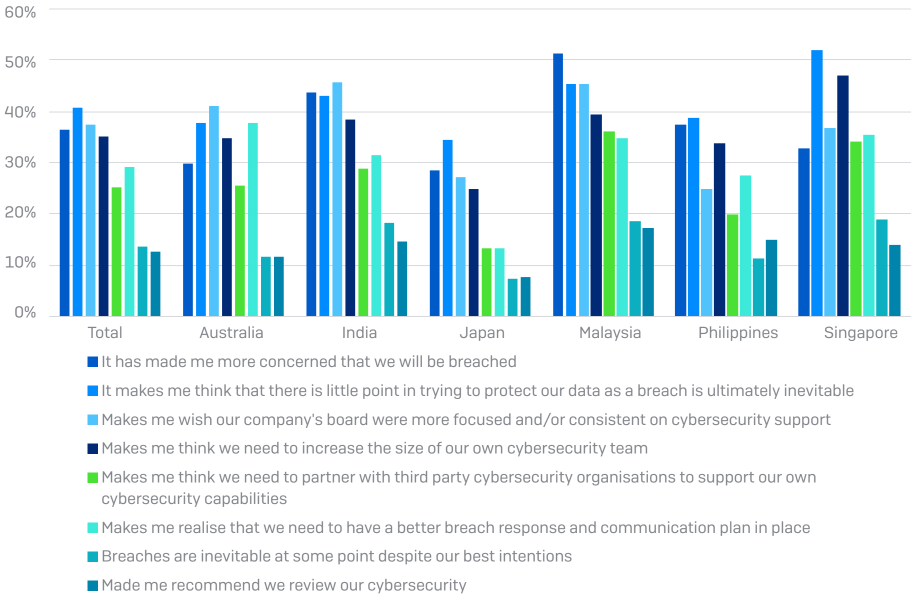
[1] By personal cyber breach we mean a cybersecurity or IT professional experiencing a loss of their own personal data as a customer of another organisation.

Has the personal experience changed the professional view?

Yes, and in some countries, quite considerably. The implications encompass aspects that impact cybersecurity fatigue and burnout, internal operations and 3rd party managed security service providers. The top 5 implications include:

1. 41% of professionals think there is little point in trying to protect company data as a breach is ultimately inevitable
2. 37% want their company's board to be more focused/and or consistent on cybersecurity issues
3. 36% are more concerned that their company will experience a breach
4. 35% feel a need to increase the size of their internal cybersecurity teams
5. 29% see a need to have an improved breach response and communication plan in place

Has the experience of having your own data compromised or lost, meant you have changed your perspective of how your own company secures its operations?



Individual country responses do see some variation across the main implications and both Malaysia and Singapore show higher levels of response rates across most categories compared to the broader group.

- Australia concentrates more upon board issues, incident response and communication plans, and the inevitability of breaches
- India shows the impact on board issues, heightened concern and the inevitability of breaches
- Japan shows overall lower levels of impact, focused on breach inevitability, heightened concern and board issues
- Malaysia leads with heightened concern, breach inevitability and board issues.
- The Philippines is concerned with breach inevitability, heightened concern and a need to increase the size of inhouse cybersecurity teams
- Lastly, Singapore is focused on breach inevitability, heightened concern and board issues

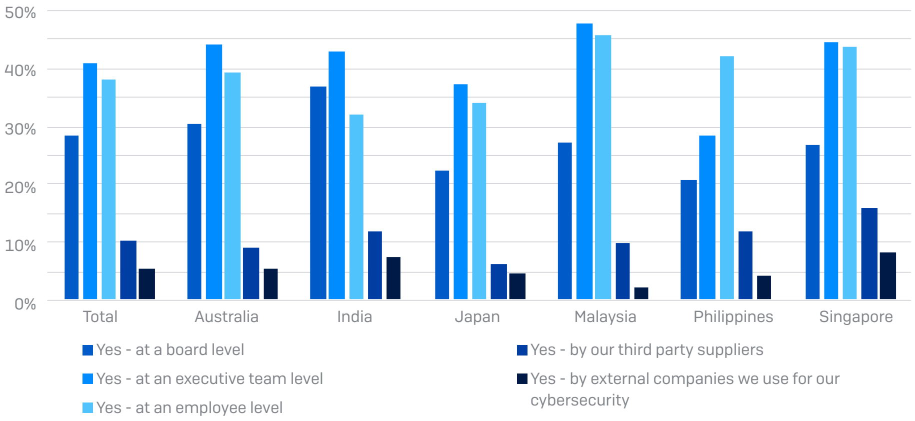
Repeat offenders and the effectiveness of education and training.

Much has been written about how human error is one of the most common contributors to a cyber breach or incident. Organisations have invested extensively in education and training for boards, SLTs, employees, and more recently as supply chain vulnerabilities have exposed companies, third party suppliers and managed security providers.

We found that despite education and training programmes, companies are experiencing lapses in cybersecurity from 'repeat offenders':

- 41% of SLTs make the same mistakes despite training and education
- 38% of employees
- 28% of boards
- 10% of third party suppliers
- 5% by third party managed cyber security providers

Does your company experience lapses in cybersecurity by employees making the same mistakes on a regular basis despite education and training?



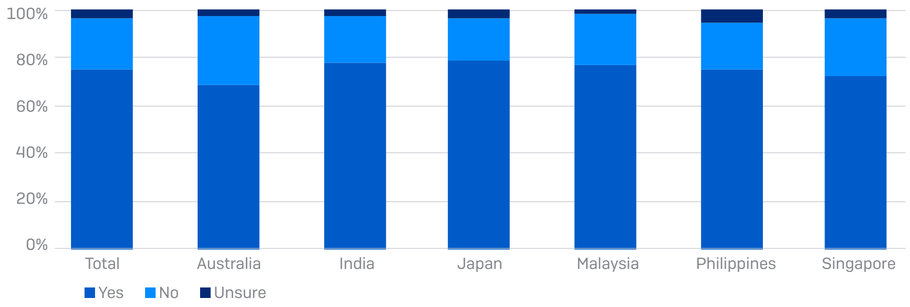
It's unrealistic to assume that an organisation can achieve and maintain a 100% error free cybersecurity environment across management, employees and partners.

What it does mean though is having an effective, tested, incident and communications plan in place is critical. So, how did our organisations fare? Pretty good for having plans, less so for response effectiveness and readiness.

Incident response plans and readiness

84% of organisations have formal cybersecurity incident response and communications plans in place. Organisations in Malaysia (92%) and India (91%) show the highest proportion of companies with plans in place, Japan (73%) and Australia (83%), the lowest.

Does your organisation have a formal cybersecurity, incident response and communications plan in place?

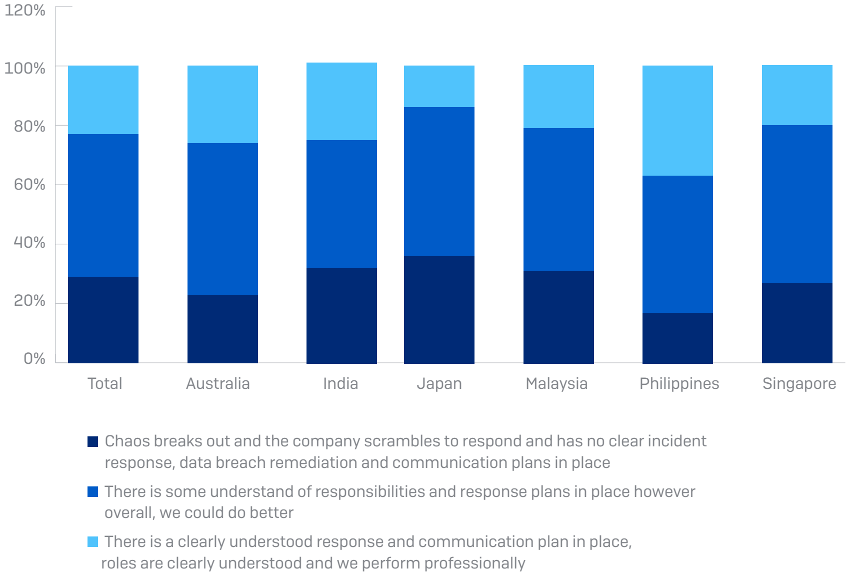


Plans in place is one thing, having an effective plan, is another.

It is telling that 75% of organisations stated their plan was initiated after their company experienced a breach. In turn, this would perhaps explain why, when asked to self-assess their company's response to a cyber-attack or breach, only 23% of companies felt "there is a clearly understand response and communication plan in place, roles are clearly understood and we perform professionally".

Conversely, 29% felt "chaos breaks out and the company scrambles to respond and has no clear incident response, data breach remediation and communication plans in place".

Which sentences best describes how your company responds, or would respond, to a cyber-attack or breach?



Data from Japan (36%) and India (32%) suggest the highest levels of 'chaos' and The Philippines (37%), Australia (26%) and India (26%) have highest levels of 'professional' execution of their plans.

It's easy to type "regularly test the plan" and most organisations no doubt strongly agree with the sentiment. However, the data suggests that either regular testing doesn't occur, or if it does, the learnings are not always incorporated into an improved version.

We would suggest that the data implies companies are struggling with building a strong, company-wide security culture. However, we weren't expecting that specific issue to top the list of frustrations organisations have with cybersecurity.

Cybersecurity and IT professionals' areas of concern and frustration

In previous reports, we have asked cybersecurity professionals what frustrates them most about their company and its cybersecurity.

This year the data shows just how dynamic the security environment can be, with multiple changes in the ranking of frustrations organisations deal with.

The top five frustrations:

1. This year establishing a strong cybersecurity culture across the company is the most significant frustration experienced. In past years, this issue ranked outside of the top 10
2. Our second frustration that cybersecurity is easy and concerns are over exaggerated rose dramatically from 10th spot in last year's list to 2nd this year.
3. Executives assume we won't be attacked dropped from 1st spot to 3rd this year, perhaps suggesting greater awareness of issues
4. Budget concerns rose from 7th to 4th, and with economic headwinds impacting many organisations, we expect to see this issue remain a top 5 concern in 2024 as well
5. SLTs pay lip service to cybersecurity jumped 3 places from 8th to 5th

Top Issues Causing Frustration	2019	2021	2022	2023
We struggle to build a strong, effective company-wide cybersecurity culture	Outside top 10	Outside top 10	Outside top 10	1
Our executives assume cybersecurity is easy and concerns are over exaggerated	3	1	10	2
Our executives assume we won't be attacked	7	7	1	3
There is not enough budget for cybersecurity	2	2	7	4
The executive team pay lip service to cybersecurity but don't believe in it	9	5	8	5
Our executives assume we will get attacked but there is nothing that can be done about it	10	8	4	6
We can't keep up with the pace of security threats	8	9	5	7
We can't employ enough cybersecurity professionals	5	3	2	8
We don't consistently prioritise cybersecurity	Outside top 10	Outside top 10	Outside top 10	9
Regulations and legislation are reactive, making managing our cybersecurity more complex	Outside top 10	Outside top 10	Outside top 10	10

The top 5 frustrations are not technology issues, nor are they regulatory and legislative problems. They are however issues with effective communication – how cybersecurity and IT professional explain cybersecurity to the greater organisation has often been anecdotally identified as a weakness across multiple areas including:

- Demystifying cybersecurity jargon to boards and SLTs
- Prioritisation of assets to protect, be they crown jewels, trinkets or baubles
- Helping identify practical steps to take in a breach

In closing

It's clear cyber fatigue and burnout are critical issues that have detrimental impacts on both employees and companies' cybersecurity capabilities. Reduced focus and higher levels of vulnerability, along with higher rates of cybersecurity and IT employee churn, are real problems for many organisations, caused by a lack of resources, executive and board pressure, and the more mundane, repetitive aspects of some cybersecurity employee roles. Technology has a role here to play through improved automation and use of a burgeoning suite of artificial intelligence (AI) cybersecurity solutions to alleviate some aspects of the causes of burnout. More critically, the data suggests building strong company-wide cybersecurity cultures, working to instil higher levels of board and SLT appreciation of the complexities of cybersecurity issues, and focusing on ensuring 'repeat cyber offenders' are coached and educated to improve their performance would help reduce many of the common cybersecurity frustrations contributing to fatigue and burnout.

The following sections of the report provide relevant data points for each of the 6 countries included in our research:

1. Australia
2. India
3. Japan
4. Malaysia
5. Philippines
6. Singapore

Country Profiles

Australia

Proportion of Cybersecurity and IT professionals experiencing cyber burnout:

- Frequently: 17% (average – 23%)
- Occasionally: 69% (average – 62%)

Have cyber burnout symptoms increased in the last 12 months?

- Significantly: 30% (average – 30%)
- Slightly: 63% (average – 60%)

Proportion of companies experiencing resignations of Cybersecurity and IT professionals due to cyber burnout:

- 22% (average – 23%)

Have staff been 'moved on' due to cyber burnout leading to performance issues?

- Yes: 16% (average – 20%)

Average hours lost per week due to cyber burnout:

- 3.8 hours / week (average – 4.1 hours / week)

Who leads cybersecurity strategy?

- IT Director
- CISO
- Cybersecurity Director or Manager

Top 3 frustrations of cybersecurity professionals:

1. We struggle to create a strong cybersecurity culture across the whole company
2. Our executives assume cybersecurity is easy and concerns are over exaggerated
3. There is not enough budget

Board and SLT understanding of cybersecurity:

Australia	Not at all	A little	Very well	Unsure
Board level	4%	41%	51%	4%
Average	7%	37%	51%	5%
SLT level	3%	39%	57%	1%
Average	6%	36%	54%	4%

Regulatory and legislative change forcing increased focus on cybersecurity at Board and SLT levels:

- Significantly: 42% (average – 44%)
- Somewhat: 55% (average – 51%)

Top 3 areas impacted by this increased focus:

1. Increased training and education
2. Investment in new / upgraded cybersecurity technologies
3. Increased cybersecurity headcount or approval for more headcount

Are regular cybersecurity briefings provided?

Yes	Board	SLT	Company-wide	3rd party suppliers	Government agencies	Customers	Informal updates	No
Australia	49%	46%	47%	21%	18%	12%	1%	1%
Average	41%	51%	45%	22%	19%	16%	2%	1%

Formal incident response plans in place:

- 83% (average – 84%)

Plan developed after an attack:

- 68% (average – 75%)

Response readiness:

- Chaos: 23% (average – 29%)
- OK but could do better: 51% (average – 48%)
- Clearly understood and perform professionally: 26% (average – 23%)

Effectiveness of training and education - % of repeat offenders:

- Board: 30% (average – 28%)
- SLT: 44% (average – 41%)
- Employees: 39% (average – 38%)

India

Proportion of Cybersecurity and IT professionals experiencing cyber burnout:

- Frequently: 37% (average – 23%)
- Occasionally: 46% (average – 62%)

Have cyber burnout symptoms increased in the last 12 months?
Significantly: 48% (average – 30%)
Slightly: 45% (average – 60%)

Proportion of companies experiencing resignations of Cybersecurity and IT professionals due to cyber burnout:

- 31% (average – 23%)

Have staff been 'moved on' due to cyber burnout leading to performance issues?

- Yes: 31% (average – 20%)

Average hours lost per week due to cyber burnout:

- 3.6 hours / week (average – 4.1 hours / week)

Who leads cybersecurity strategy?

- IT Director or Manager
- Cybersecurity Director or Manager
- CIO/CTO

Top 3 frustrations of cybersecurity professionals:

1. Our executives assume cybersecurity is easy and concerns are over exaggerated
2. Our executives assume we will never get attacked
3. We struggle to create a strong cybersecurity culture across the whole company

Board and SLT understanding of cybersecurity:

India	Not at all	A little	Very well	Unsure
Board level	4%	31%	58%	6%
Average	7%	37%	51%	5%
SLT level	4%	26%	66%	4%
Average	6%	36%	54%	4%

Regulatory and legislative change forcing increased focus on cybersecurity at Board and SLT levels:

- Significantly: 59% (average – 44%)
- Somewhat: 37% (average – 51%)

Top 3 areas impacted by this increased focus:

1. Increased training and education for IT/Cybersecurity employees only
2. Increased training and education for all employees
3. Increase in cybersecurity headcount or approval for new headcount

Are regular cybersecurity briefings provided?

Yes	Board	SLT	Company-wide	3rd party suppliers	Government agencies	Customers	Informal updates	No
India	46%	53%	48%	27%	26%	21%	0%	0%
Average	41%	51%	45%	22%	19%	16%	2%	1%

Formal incident response plans in place:

- 91% (average – 84%)

Plan developed after an attack:

- 78% (average – 75%)

Response readiness:

- Chaos: 32% (average – 29%)
- OK but could do better: 43% (average – 48%)
- Clearly understood and perform professionally: 26% (average – 23%)

Effectiveness of training and education - % of repeat offenders:

- Board: 37% (average – 28%)
- SLT: 43% (average – 41%)
- Employees: 32% (average – 38%)

Japan

Proportion of Cybersecurity and IT professionals experiencing cyber burnout:

- Frequently: 23% (average – 23%)
- Occasionally: 46% (average – 62%)

Have cyber burnout symptoms increased in the last 12 months?

- Significantly: 38% (average – 30%)
- Slightly: 58% (average – 60%)

Proportion of companies experiencing resignations of Cybersecurity and IT professionals due to cyber burnout:

- 13% (average – 23%)

Have staff been 'moved on' due to cyber burnout leading to performance issues?

- Yes: 12% (average – 20%)

Average hours lost per week due to cyber burnout:

- 3.6 hours / week (average – 4.1 hours / week)

Who leads cybersecurity strategy?

- Cybersecurity Director or Manager
- CISO
- CIO/CTO

Top 3 frustrations of cybersecurity professionals:

1. The executive team pay lip service to cybersecurity but don't truly believe in it
2. Our executives assume we will never get attacked
3. We struggle to create a strong cybersecurity culture across the whole company

Board and SLT understanding of cybersecurity:

Japan	Not at all	A little	Very well	Unsure
Board level	18%	36%	38%	8%
Average	7%	37%	51%	5%
SLT level	14%	47%	32%	6%
Average	6%	36%	54%	4%

Regulatory and legislative change forcing increased focus on cybersecurity at Board and SLT levels:
Significantly: 28% (average – 44%)
Somewhat: 60% (average – 51%)

Top 3 areas impacted by this increased focus:

1. Increased training and education for all employees
2. Investment in new / upgraded cybersecurity technologies
3. Increased training and education for IT/cybersecurity employees only

Are regular cybersecurity briefings provided?

Yes	Board	SLT	Company-wide	3rd party suppliers	Government agencies	Customers	Informal updates	No
Japan	21%	38%	36%	13%	4%	12%	5%	1%
Average	41%	51%	45%	22%	19%	16%	2%	1%

Formal incident response plans in place:

- 73% (average – 84%)

Plan developed after an attack:

- 79% (average – 75%)

Response readiness:

- Chaos: 36% (average – 29%)
- OK but could do better: 50% (average – 48%)
- Clearly understood and perform professionally: 14% (average – 23%)

Effectiveness of training and education - % of repeat offenders:

- Board: 22% (average – 28%)
- SLT: 37% (average – 41%)
- Employees: 34% (average – 38%)

Malaysia

Proportion of Cybersecurity and IT professionals experiencing cyber burnout:

- Frequently: 21% (average – 23%)
- Occasionally: 71% (average – 62%)

Have cyber burnout symptoms increased in the last 12 months?

- Significantly: 29% (average – 30%)
- Slightly: 61% (average – 60%)

Proportion of companies experiencing resignations of Cybersecurity and IT professionals due to cyber burnout:

- 25% (average – 23%)

Have staff been 'moved on' due to cyber burnout leading to performance issues?

- Yes: 23% (average – 20%)

Average hours lost per week due to cyber burnout:

- 4.1 hours / week (average – 4.1 hours / week)

Who leads cybersecurity strategy?

- Cybersecurity Director or Manager
- IT Director or Manager
- CISO

Top 3 frustrations of cybersecurity professionals:

1. We struggle to create a strong cybersecurity culture across the whole company
2. Our executives assume cybersecurity is easy and concerns are over exaggerated
3. It is hard to keep up with the pace of cybersecurity threats

Board and SLT understanding of cybersecurity:

Malaysia	Not at all	A little	Very well	Unsure
Board level	3%	42%	52%	3%
Average	7%	37%	51%	5%
SLT level	2%	35%	60%	4%
Average	6%	36%	54%	4%

Regulatory and legislative change forcing increased focus on cybersecurity at Board and SLT levels:

- Significantly: 45% (average – 44%)
- Somewhat: 53% (average – 51%)

Top 3 areas impacted by this increased focus:

1. We struggle to create a strong cybersecurity culture across the whole company
2. Our executives assume cybersecurity is easy and concerns are over exaggerated
3. It is hard to keep up with the pace of cybersecurity threats

Are regular cybersecurity briefings provided?

Yes	Board	SLT	Company-wide	3rd party suppliers	Government agencies	Customers	Informal updates	No
Malaysia	49%	65%	56%	29%	33%	20%	1%	0%
Average	41%	51%	45%	22%	19%	16%	2%	1%

Formal incident response plans in place:

- 92% (average – 84%)

Plan developed after an attack:

- 77% (average – 75%)

Response readiness:

- Chaos: 31% (average – 29%)
- OK but could do better: 48% (average – 48%)
- Clearly understood and perform professionally: 21% (average – 23%)

Effectiveness of training and education - % of repeat offenders:

- Board: 27% (average – 28%)
- SLT: 47% (average – 41%)
- Employees: 45% (average – 38%)

The Philippines

Proportion of Cybersecurity and IT professionals experiencing cyber burnout:

- Frequently: 23% (average – 23%)
- Occasionally: 71% (average – 62%)

Have cyber burnout symptoms increased in the last 12 months?

- Significantly: 21% (average – 30%)
- Slightly: 67% (average – 60%)

Proportion of companies experiencing resignations of Cybersecurity and IT professionals due to cyber burnout:

- 17% (average – 23%)

Have staff been 'moved on' due to cyber burnout leading to performance issues?

- Yes: 13% (average – 20%)

Average hours lost per week due to cyber burnout:

- 4.6 hours / week (average – 4.1 hours / week)

Who leads cybersecurity strategy?

- Cybersecurity Director or Manager
- IT Director or Manager
- CIO/CTO

Top 3 frustrations of cybersecurity professionals:

1. Our executives assume we will never get attacked
2. Our executives assume cybersecurity is easy and concerns are over exaggerated
3. We struggle to create a strong cybersecurity culture across the whole company

Board and SLT understanding of cybersecurity:

Philippines	Not at all	A little	Very well	Unsure
Board level	3%	40%	56%	1%
Average	7%	37%	51%	5%
SLT level	4%	34%	59%	3%
Average	6%	36%	54%	4%

Regulatory and legislative change forcing increased focus on cybersecurity at Board and SLT levels:

- Significantly: 50% (average – 44%)
- Somewhat: 49% (average – 51%)

Top 3 areas impacted by this increased focus:

1. Increase in training and education for all employees
2. Increase in training and education for IT/cybersecurity employees
3. Investment in new/upgraded cybersecurity technologies

Are regular cybersecurity briefings provided?

Yes	Board	SLT	Company-wide	3rd party suppliers	Government agencies	Customers	Informal updates	No
Philippines	52%	60%	41%	25%	11%	13%	4%	1%
Average	41%	51%	45%	22%	19%	16%	2%	1%

Formal incident response plans in place:

- 88% (average – 84%)

Plan developed after an attack:

- 75% (average – 75%)

Response readiness:

- Chaos: 17% (average – 29%)
- OK but could do better: 46% (average – 48%)
- Clearly understood and perform professionally: 37% (average – 23%)

Effectiveness of training and education - % of repeat offenders:

- Board: 20% (average – 28%)
- SLT: 28% (average – 41%)
- Employees: 42% (average – 38%)

Singapore

Proportion of Cybersecurity and IT professionals experiencing cyber burnout:

- Frequently: 16% (average – 23%)
- Occasionally: 72% (average – 62%)

Have cyber burnout symptoms increased in the last 12 months?

- Significantly: 18% (average – 30%)
- Slightly: 64% (average – 60%)

Proportion of companies experiencing resignations of Cybersecurity and IT professionals due to cyber burnout:

- 38% (average – 23%)

Have staff been 'moved on' due to cyber burnout leading to performance issues?

- Yes: 26% (average – 20%)

Average hours lost per week due to cyber burnout:

- 4.2 hours / week (average – 4.1 hours / week)

Who leads cybersecurity strategy?

- IT Director or Manager
- Cybersecurity Director or Manager
- CIO/CTO

Top 3 frustrations of cybersecurity professionals:

1. We struggle to create a strong cybersecurity culture across the whole company
2. Our executives assume cybersecurity is easy and concerns are over exaggerated
3. It is hard to keep up with the pace of cybersecurity

Board and SLT understanding of cybersecurity:

Singapore	Not at all	A little	Very well	Unsure
Board level	7%	33%	57%	3%
Average	7%	37%	51%	5%
SLT level	5%	32%	58%	5%
Average	6%	36%	54%	4%

Regulatory and legislative change forcing increased focus on cybersecurity at Board and SLT levels:

- Significantly: 42% (average – 44%)
- Somewhat: 52% (average – 51%)

Top 3 areas impacted by this increased focus:

1. Investment in new/upgraded cybersecurity technologies
2. Increase in training and education for all employees
3. Increase in training and education for IT/cybersecurity employees

Are regular cybersecurity briefings provided?

Yes	Board	SLT	Company-wide	3rd party suppliers	Government agencies	Customers	Informal updates	No
Singapore	38%	58%	51%	25%	29%	24%	3%	0%
Average	41%	51%	45%	22%	19%	16%	2%	1%

Formal incident response plans in place:

- 85% (average – 84%)

Plan developed after an attack:

- 72% (average – 75%)

Response readiness:

- Chaos: 27% (average – 29%)
- OK but could do better: 53% (average – 48%)
- Clearly understood and perform professionally: 20% (average – 23%)

Effectiveness of training and education - % of repeat offenders:

- Board: 26% (average – 28%)
- SLT: 44% (average – 41%)
- Employees: 43% (average – 38%)

The Sophos Perspective

"All work and no play makes Jackie dev/null"

Aaron Bugal, Field CTO, Asia Pacific and Japan

Cybersecurity is a surging industry – a beckoning light drawing in many new practitioners wanting to make a difference.

But like moths to a flame, many aren't sure what is drawing them in.

"I want to be in cybersecurity!" they say.

This is great but there are so many aspects to effective cybersecurity. Analysing malware. Forensic recovery. System hardening. Policy writing. Team leadership. This is just a small sub-set of what the cybersecurity industry needs and expecting to be a generalist across all of these and more will quickly equate to a very overwhelmed employee.

And the cracks are starting to show.

But it's not the employees' fault. As organisations scramble to respond to cyber criminals and their exploits of dragging high profile organisations through the grinder for lax defences, it's no wonder they're scooping up anyone who says, 'I want to be in cybersecurity'.

Many of these newly minted professionals may be unaware of the technical and non-technical roles that exist and the specialisations within each that enable an effective cyber defence force.

The slowness of developing (sometimes even no development), a cybersecurity culture within an organisation equates to not getting the right set of skills for the gaps that are present. While blame isn't solely that of business owners – accountability is.

The threat landscape and everything about cybersecurity has exploded exponentially in the last few years. However, business owners and those who drive company decisions must accept the accountability of their inability and/or inaction if they ever become a victim of a cyber attack.

This report's vast insight to organisational cyber stress urges us to change. Although there's not a simple fix, an attitude adjustment would go a long way in defining the right expectations around what it means to evolve into a cyber resilient business. Boards and executive committees need to drive change and demand responsibility from their deputised charges, in essence, better governance around cyber approaches. However, they need to clearly articulate their accountability in developing and maintaining a plan - although cyber security is a team sport, the buck stops (and starts) at the top.

Appendix

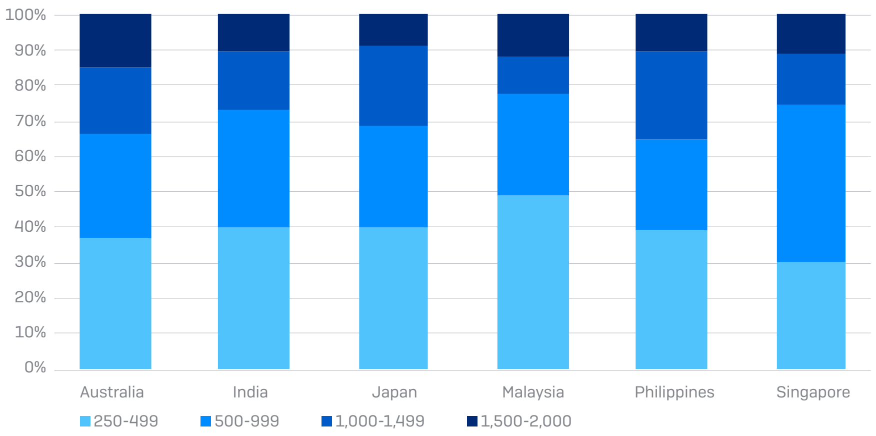
Survey Demographics and Methodology

In September 2023, Sophos commissioned Tech Research Asia (TRA) to undertake research into the Asia Pacific and Japan cybersecurity landscape. This included a major quantitative component with a total of 919 responses captured from Australia (204 companies), India (202), Japan (204), Malaysia (104), The Philippines (103) and Singapore (102).

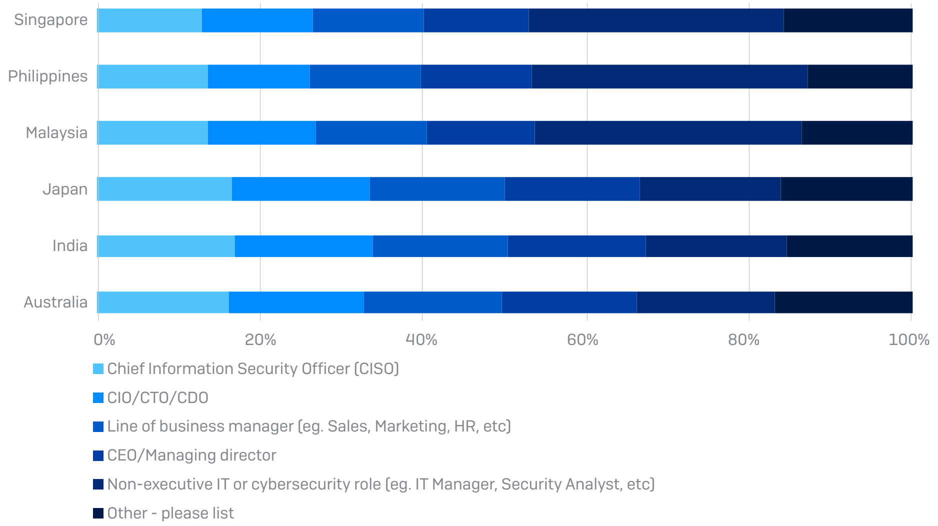
Respondents completed an anonymous, online survey. The survey incorporated responses from cybersecurity and IT employees to provide data on the personal impact of cyber burnout.

The following charts provide more detail about company size, respondent role and industry sector.

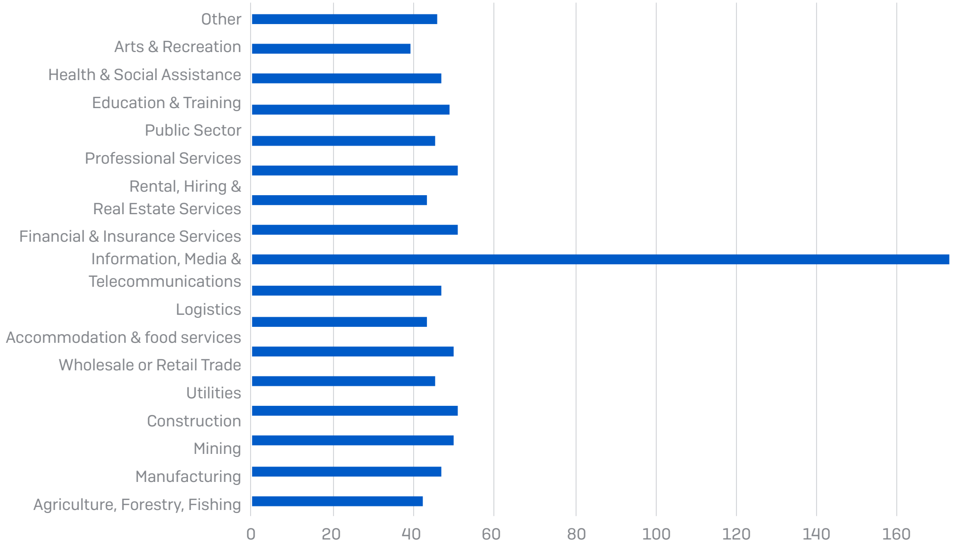
How many people work at your company?



Respondents by Role and Country



Respondents by Industry Sector



About Sophos

Sophos is a worldwide leader in next-generation cybersecurity, protecting more than 500,000 organisations and millions of consumers in more than 150 countries from today's most advanced cyberthreats. Powered by threat intelligence, AI and machine learning from SophosLabs and SophosAI, Sophos delivers a broad portfolio of advanced products and services to secure users, networks and endpoints against ransomware, malware, exploits, phishing and the wide range of other cyberattacks. Sophos provides a single integrated cloud-based management console, Sophos Central – the centerpiece of an adaptive cybersecurity ecosystem that features a centralised data lake that leverages a rich set of open APIs available to customers, partners, developers, and other cybersecurity vendors. Sophos sells its products and services 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

Tech Research Asia (TRA) is a technology research, consulting and advisory firm working across Asia Pacific specialising in analysing trends in technology and the impact on business value. We help organisations across the region, technology vendors and channel partners build deeper market understanding and improve their business results.

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

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

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

Registered in England and Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK

SOPHOS