proofpoint.

REPORT

Asia-Pacific

2023 State of the Phish

An in-depth exploration of user awareness, vulnerability and resilience

proofpoint.com

A COMMISSIONED SURVEY OF:

7,500
working adults across 15 countries

1,050
IT security professionals across those countries

AND:

135 million
simulated phishing attacks sent by our customers over a 12-month period

18 million
emails reported by our customers' end users over a 12-month period

2022: Cyber Criminals Get Even More Creative

Every year, threat actors look for new ways to outwit victims and bypass defenses. And 2022 was no different. As businesses rolled out new security controls, cyber criminals responded.

They added complex techniques like telephone-oriented attack delivery and multi-factor authentication (MFA) bypass. Unknown to most users, these techniques gave cyber attackers a new advantage. And with threat actors constantly upping their game, CISOs and infosec teams had their work cut out.

Now in its ninth year, our annual *State of the Phish* report explores end-user security awareness, resilience and risk using survey data from 15 countries, along with data sourced from our products and threat research team. The report benchmarks understanding of common cyber attacks and defensive tactics, before looking at how potential gaps in knowledge and cyber hygiene enable the real-world attack landscape. Most attacks target people before they target systems. That's why helping users build good security habits is crucial. So, the final section of the report examines security awareness practices and outlines opportunities to build and sustain a security-aware culture at every level of an organisation.

Alongside this year's main report, we're also giving regional summaries to help organisations understand how local nuances affect gaps in awareness. This regional summary includes data from **Australia, Japan, Singapore and South Korea**. Data has been drawn from surveys of 2,000 working adults and 200 security.

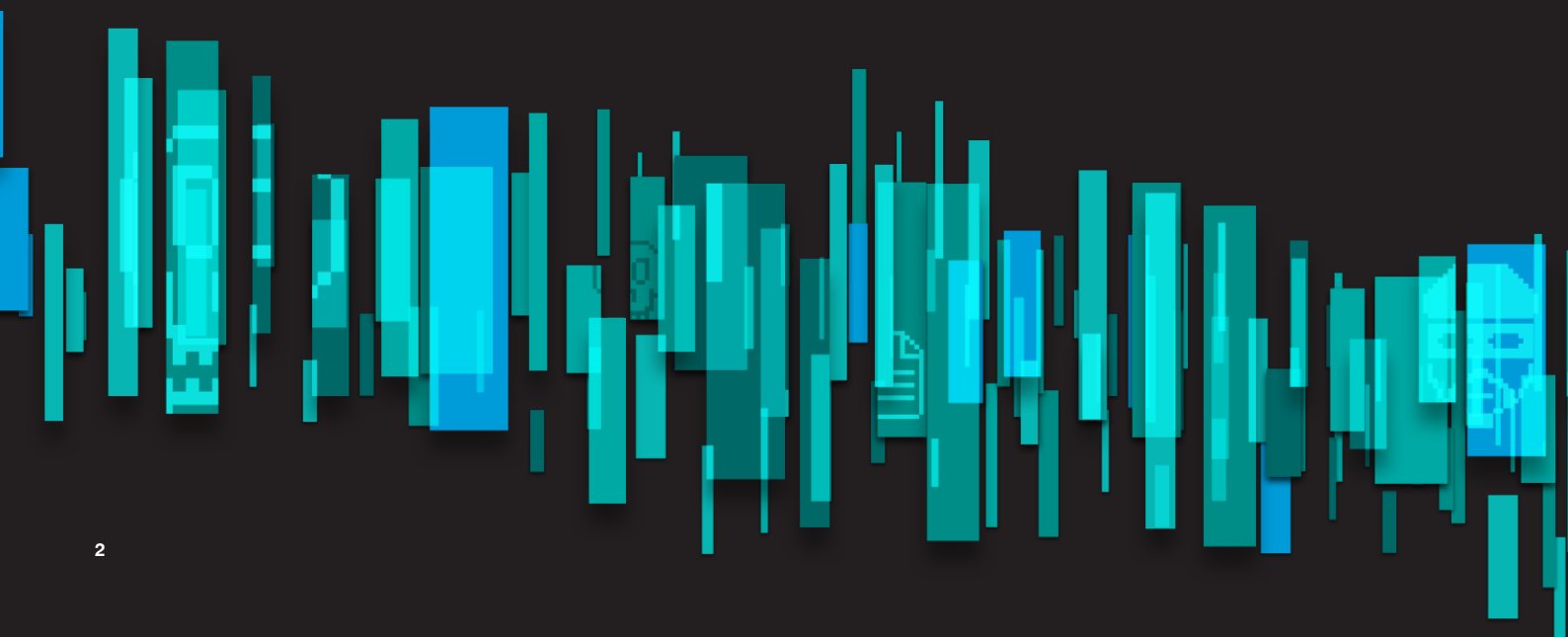
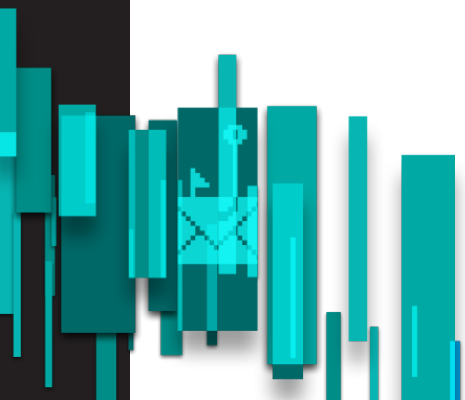


TABLE OF CONTENTS



Key Findings: Global

44%

of people think an email is safe when it contains familiar branding

$300K-400K

telephone-oriented attack delivery attempts daily, with a peak of 600k per day in August 2022

1/3

of people took a risky action (such as clicking links or downloading malware) when faced with an attack

increase in direct financial loss from successful phishing

30 Million

malicious messages sent in 2022 involved Microsoft branding or products

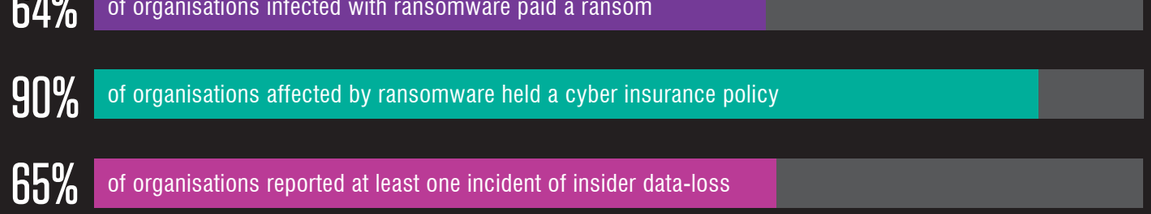
> 1 in 10

threats were blocked as a result of user reporting

can't define "malware," "phishing" and "ransomware"

Even basic concepts are misunderstood

ONLY **35%** of organisations conduct phishing simulations



ONLY **56%** of organisations with a security awareness program train all their employees

of security professionals consider security a top priority at their company

VS.

of employees say cybersecurity is not a top priority of theirs at work

64%

of Japanese organisations were likely to suffer a successful phishing attack—20% lower than globally

94% and 80%

of Australian organisations were most likely to experience successful phishing attacks and supply chain attacks, respectively

Spotlight on Asia-Pacific

There were significant variations between all 15 countries surveyed for *State of the Phish*—as you might expect when different languages, cultures and levels of digital maturity are involved. And this also played out between the four countries in this summary.

With multiple financial centres and a reputation for innovation, the countries of the Asia-Pacific and Japan (APJ) region present a rich set of targets for cyber criminals. But cultural and language barriers make some more susceptible to certain threat types than others.

Japanese organisations were least likely to suffer a successful phishing attack, at 64% compared to 84% globally. Our hypothesis for why this might be comes down to cyber criminals lacking familiarity with the Japanese language. This could make it easier for Japanese employees to spot poorly worded lures. But even if this is the case, businesses will still want to ensure they have the right tools in place to measure malicious activity.

Within the region, Australian organisations were most likely to experience both successful phishing (94% vs 84% global average) and supply chain attacks (80% vs 69% global). Australia is a mature digital market, with almost 100% of adults able to access the internet. This large digital footprint could explain the higher levels of attack. Australian law also requires disclosure of any breach in which personal information is accessed or lost, which could also lead to more self-reporting.

Of course, these outliers are likely to be the result of several factors. Around the world, English is the language most used in phishing attacks, so business that don't conduct activity in English may receive some protection. Similarly, in some countries it may be less culturally acceptable to admit to a security breach, leading to under-reporting. And with a global cybersecurity talent shortage, some organisations might struggle to recruit the experts they need to remediate all the threats they face.

COMING TO TERMS:

Even basic concepts are still not fully understood—more than a third can't define "malware," "phishing" and "ransomware."

40%

of users know what ransomware is, a 9-point jump from 2019—the biggest increase among the terms we asked about

29% and 30%

of users knew the relatively new terms smishing and vishing, respectively

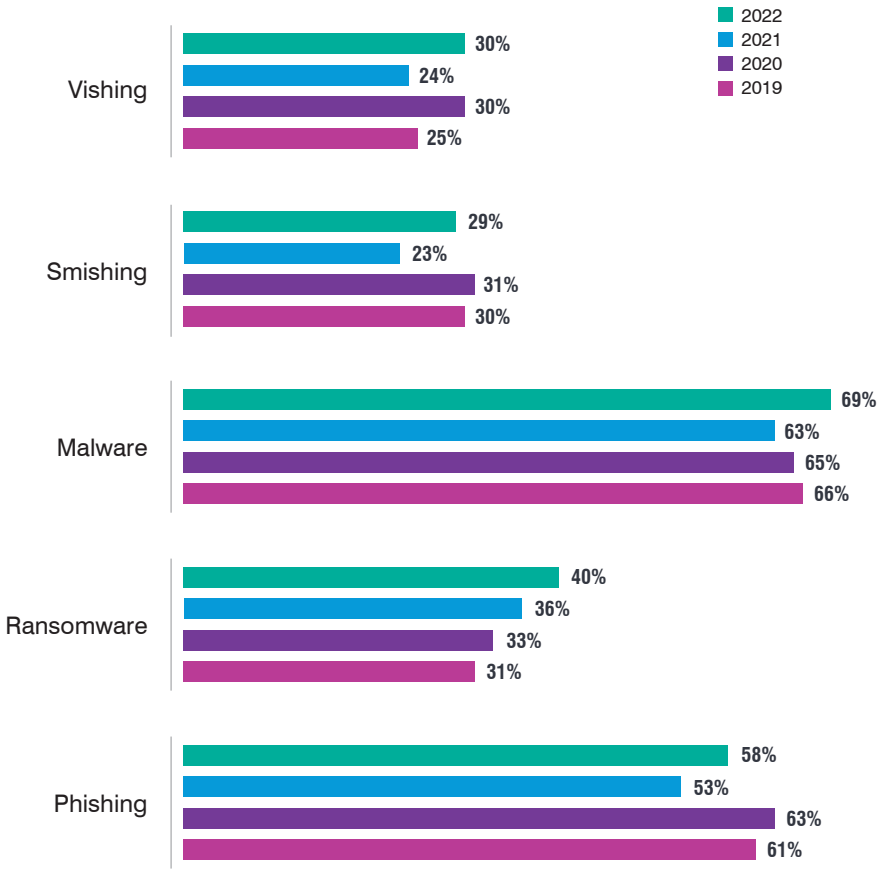
58%

of users knew what phishing is, a 5-point increase from last year but 3 points below 2019

Security awareness: insights and opportunities

Across the 15 surveyed countries globally, a similar pattern appears when we look at end-user knowledge of basic security terms. Common threats such as phishing, ransomware and malware have been around for years, but people still don't fully understand what they are. And there is even less awareness of newer threats such as smishing (SMS phishing) and vishing (voice phishing). Disappointingly, our data shows little change year on year. One reason for this may be that while most organisations have a security awareness program, not every organisation provides training to everyone within the organisation.

End-User Understanding Shows Little Change from Year to Year



THE UNCERTAINTY PRINCIPLE:

72%

of Japanese users knew what phishing is, a notably higher percentage than the three other Asia-Pacific countries surveyed

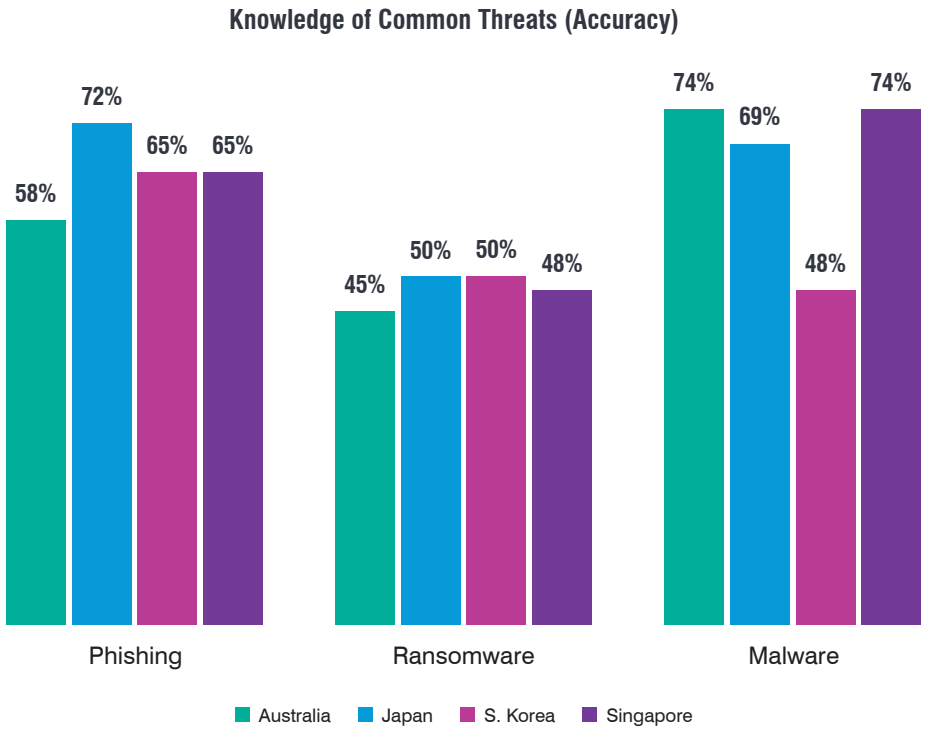
50%

of Japanese and South Korean users were familiar with ransomware, slightly higher than the other two countries

74%

of Australian and Singaporean users knew what malware is, the highest among the four Asia-Pacific countries we surveyed

Reviewing the three most common attack types for this summary reveals that understanding of these terms is more or less equal between countries in the region.



One explanation for the variations that do exist could be that use of security awareness programs varies between the four countries. Singaporean organisations were the most likely to cover common threats in their training. This is possibly the result of public awareness of phishing increasing after a series of high-profile attacks in recent years.

TOPICAL TRAINING:

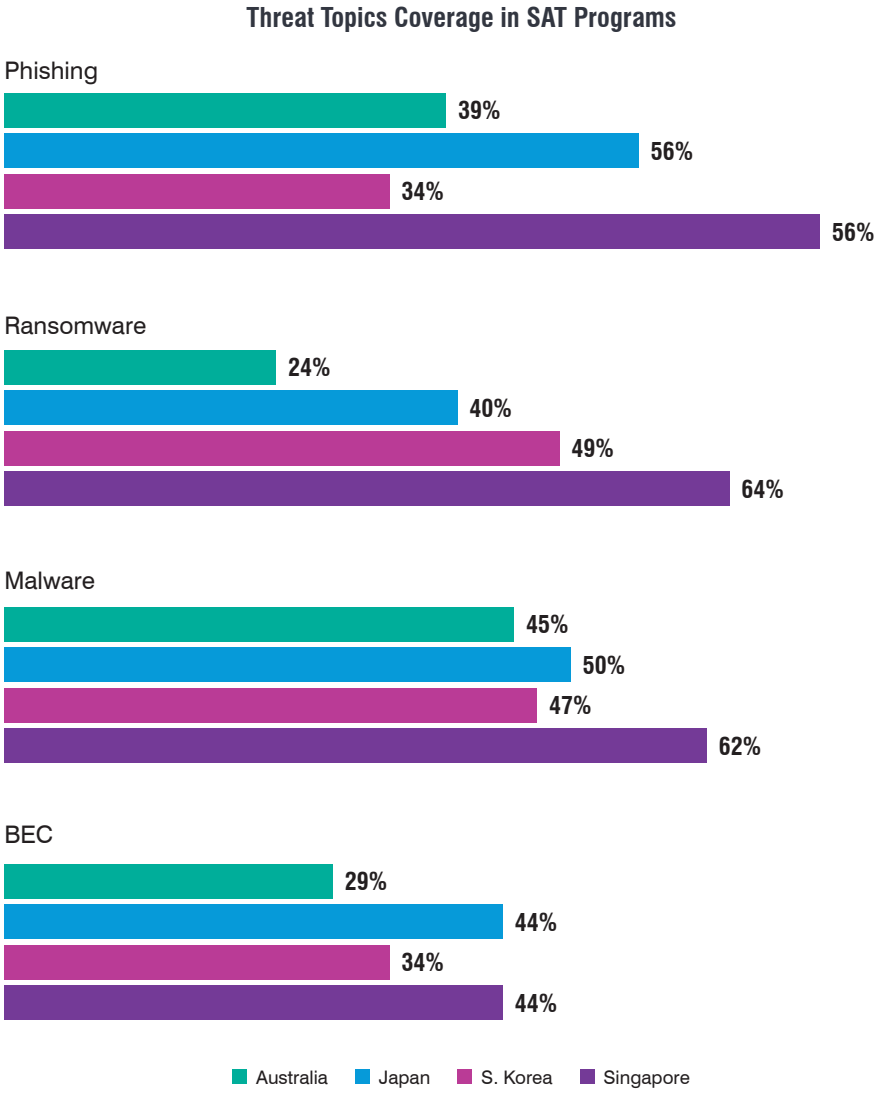
Singaporean organisations were the most likely among the four Asia-Pacific countries we surveyed to cover common cyber threats in their security awareness programs

56%
covered phishing

64%
covered ransomware

62%
covered malware

44%
covered BEC (tied with Japan)



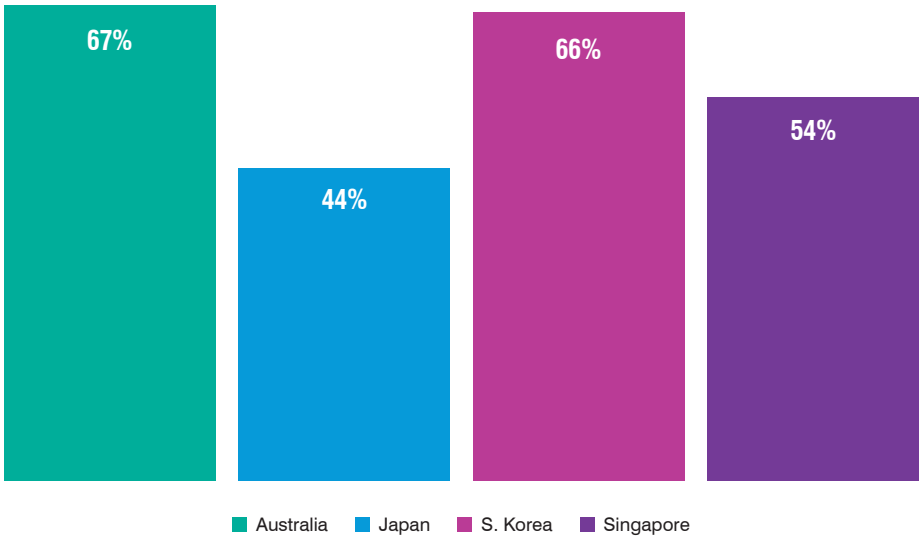
AWARENESS FOR ALL:

67%

of Australian organisations trained all of their workforce in security awareness, the highest among the Asia-Pacific countries in our survey

Australia and South Korea both do well in terms of offering training to everyone in a given organisation, outperforming the global average. But with cyber criminals always looking for new routes into target organisations, it's crucial that everyone participates in security awareness programs.

Percentage of Organisations That Trained Everyone in Their Security Awareness Programs



TRAINING TYPES:

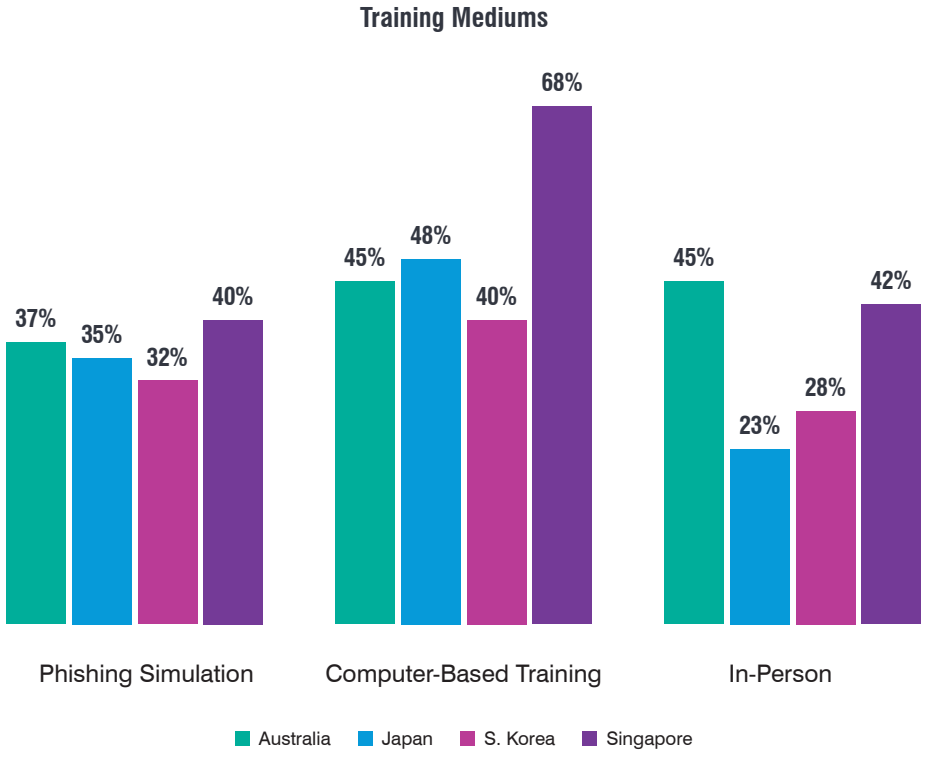
68%

of Singaporean organisations offered computer-based training, well above rates in other APAC countries surveyed. The island city-state also led in phishing simulations

45%

of Australian organisations offered in-person training, the highest percentage among surveyed countries in the Asia-Pacific region

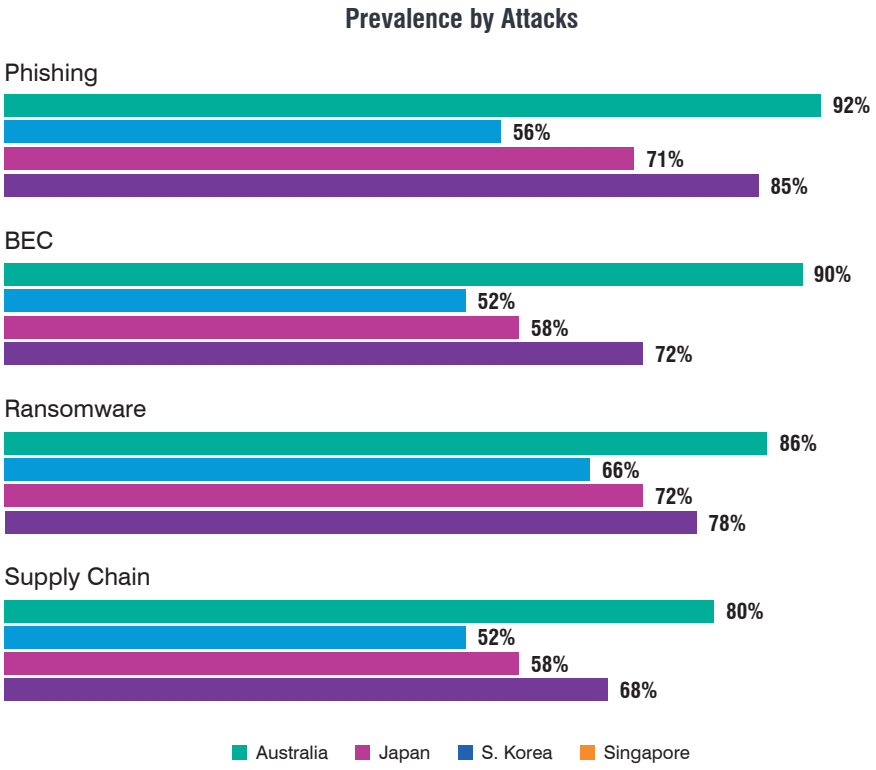
Notably, use of phishing simulation was similar in all four countries. It ranged between 32% and 40%, meaning most organisations aren't taking advantage of this practical and memorable form of training.



A smaller percentage of South Korea organisations reported phishing, BEC, ransomware and supply-chain attacks among the Asia-Pacific countries we surveyed. The opposite was true for Australian organisations, which reported the highest percentage of all four types of attack.

Threat Landscape Trends

As a mature, English-speaking market, Australia faced higher prevalence of all four major attack types: phishing, business email compromise, ransomware and supply-chain attacks. The four countries ranked identically for all attacks, possibly because of the language and digital maturity considerations described above.



PAYING UP (OR NOT):

90%

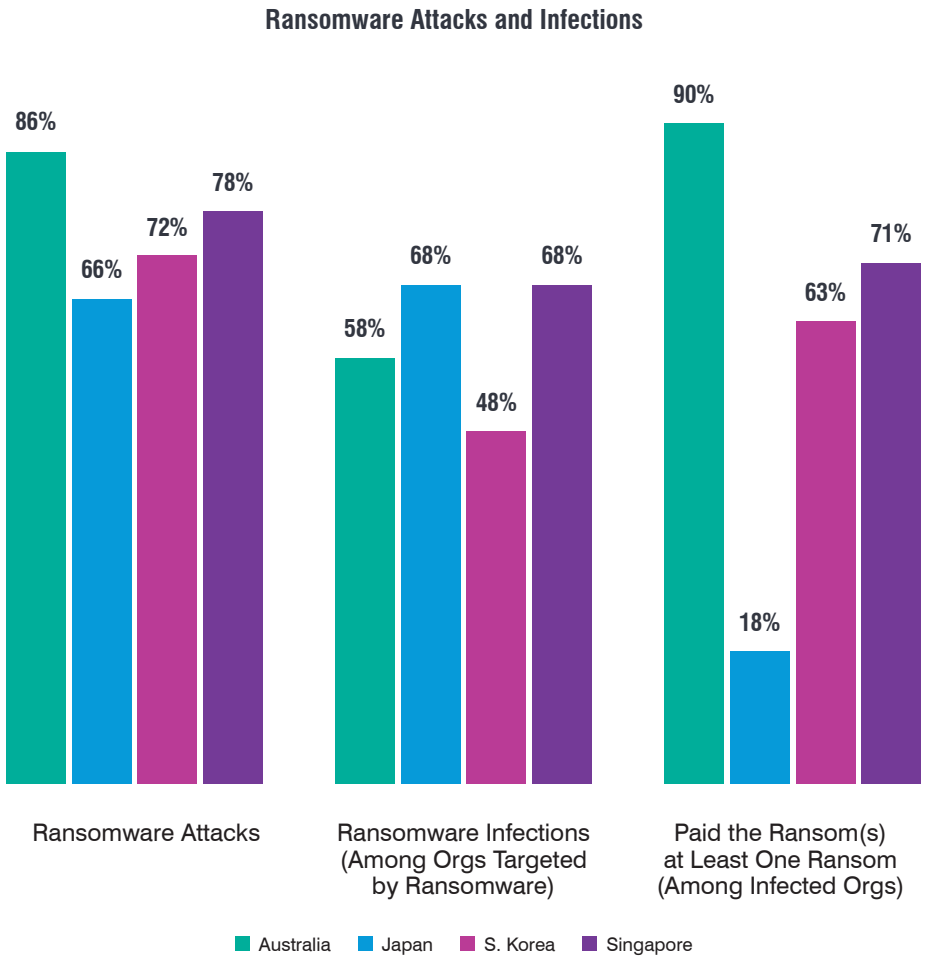
of Australian organisations hit by ransomware chose to pay

18%

of Japanese organisations hit by ransomware chose to pay

Ransomware: attacks and infections are widespread

Ransomware is a common follow-on attack after malware infection. All four countries showed a high probability of attempted ransomware delivery. Where differences emerged was in their willingness to pay.



RANSOMWARE REIMBURSEMENTS:

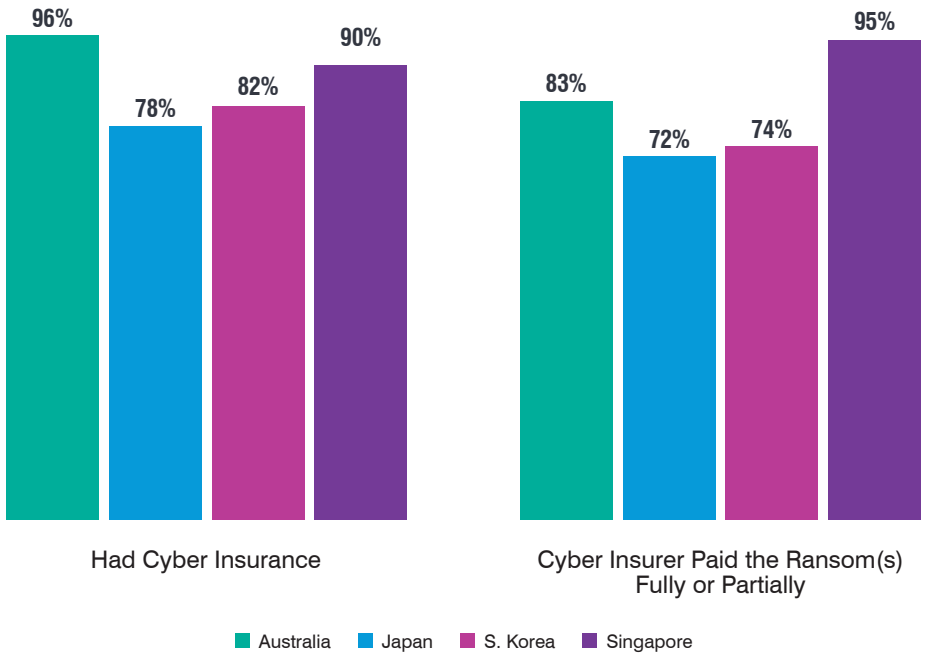
90%+

of Australian and Singaporean organisations say they have cyber insurance. But Australian insurers were significantly less likely to help pay ransomware demands.

Japanese organisations were globally the least likely to pay, with just 18% saying that they paid vs. a 64% global average. Japanese law prohibits companies from giving money to organised crime; it may be that cyber crime is treated as such by most organisations. Conversely, 90% of Australian organisations hit by ransomware chose to pay. As payments reward and reinforce criminal behaviour, the Australian government and several others around the world are considering making ransomware payment illegal.

Use of cyber insurance mapped closely to the likelihood of ransomware attack, with more than 90% of Australian and Singaporean organisations saying they have it.

Role of Cyber Insurers (Among Orgs Affected by Ransomware)



Recommendations

With so much variation between markets and businesses, an individual security program tailored to real-life threats and user risk is the ideal. But if you aren't quite there yet, this year's *State of the Phish* suggests a few helpful approaches.

Reduce complexity by asking the right questions.

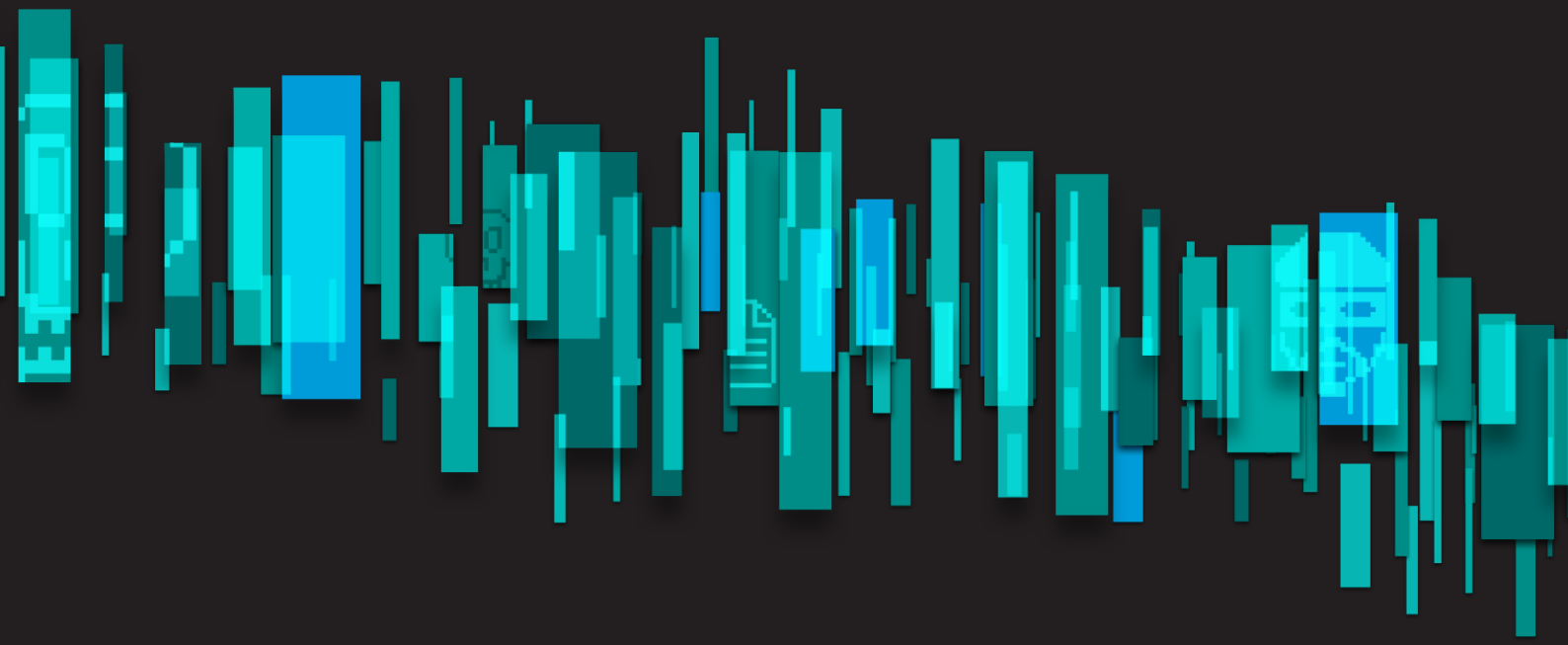
- Who in my organisation is being attacked?
- Where are the current defensive gaps?
- What are my priorities to mitigate human risk?

Pair threat intelligence with organisation-wide security awareness education.

- Identify which users are most likely to be targeted and who is most likely to succumb.
- Match training content to threats currently circulating.
- Train people to recognise phishing using the lures targeting them.

Build a security culture that goes beyond training and compliance.

- Training is crucial but not sufficient.
- A strong workplace security culture will encourage users to take information security more seriously in their personal lives.
- Measure the metrics that matter and respond with appropriate and fair remediation.



LEARN MORE

To learn more about how Proofpoint provides insight into your user risks and helps you mitigate them with a people-centric cybersecurity strategy, visit **proofpoint.com.**

ABOUT PROOFPOINT

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including 75 percent of the Fortune 100, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at **www.proofpoint.com**

proofpoint.

0400-012-02-01