proofpoint

Asia-Pacific and Japan

REPORT

2024 State of the Phish

Risky actions, real-world threats and user resilience in an age of human-centric cybersecurity

proofpoint.com

INTRODUCTION

According to our annual *State of the Phish* report, most users in the Asia-Pacific and Japan (APJ) aren't sure if security is their responsibility or someone else's. And this lack of clarity can have significant consequences; our data shows stark correlations between attitudes and outcomes across the region.

Every day, APJ users make choices between security and convenience. And this regional summary shows that most of the time they favor the latter. In the following pages we'll take a closer look at the attitudes of both security professionals and end users, as well as some key threat trends. And we'll end with suggestions that should help people change their behaviour and start putting security first.

TABLE OF CONTENTS

Key Findings: Global

Over 1 million

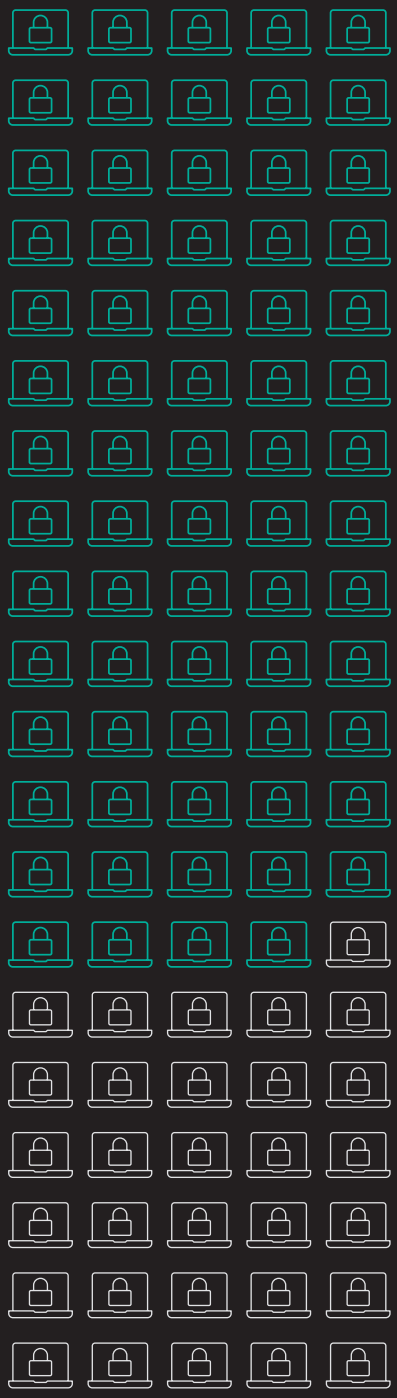
attacks are launched with MFA-bypass framework EvilProxy every month, but 89% of security professionals still believe MFA provides complete protection against account takeover.

of users took a risky action

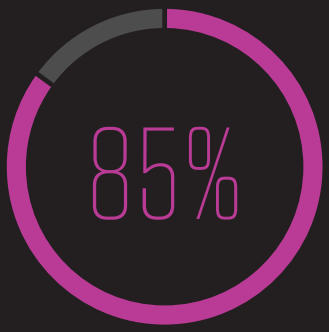
of them knew they were doing something risky

66 million

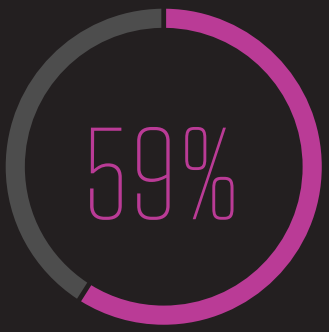
BEC attacks were detected and blocked on average per month by Proofpoint.



69% of organisations were infected by ransomware.



of security professionals said that most employees know they are responsible for security, but



of users either weren't sure or claimed that they're not responsible at all.

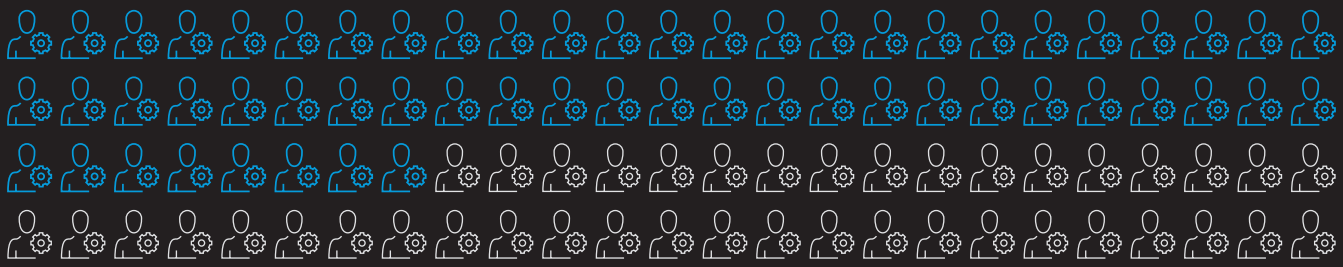
10 million

telephone-oriented attack delivery (TOAD) messages are sent every month.

Microsoft continues to be the most abused brand, with

68 million

malicious messages associated with the brand or its products.



58% of users who took risky actions engaged in behaviour that would have made them vulnerable to common social engineering tactics.

Spotlight on Asia-Pacific and Japan

This year's *State of the Phish* surveyed 7,500 users and 1,050 security professionals in 15 countries. This APJ regional summary includes data from **Australia, Japan, South Korea and Singapore**. (Our global report offers a comparative view of all 15 countries.)

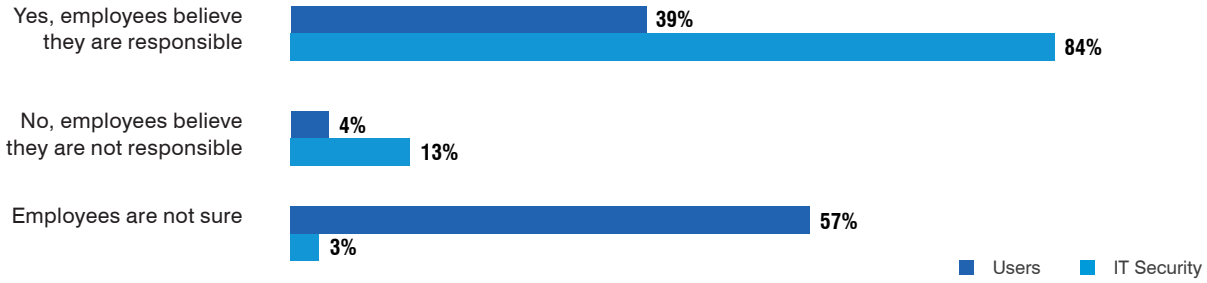
There were significant variations between all 15 countries surveyed for *State of the Phish*—as you might expect when different languages, cultures and levels of digital maturity are involved. And this also played out between the four countries in this summary.

But in at least one respect the APJ region shows some uniformity. Users are more likely to say they are unsure about their responsibility for security (57% vs 54% global average). And their uncertainty may have an impact on how they behave. On average, they take far fewer risks than the global average (63% vs 71%). Yet when users do take risks, they're more likely to know their action comes with risks (98% vs 95% global average).

At the country level, only 28% of users in South Korea believe that security is their responsibility, which is much lower than the global average (41%). This attitude may be part of the reason that South Korea has the highest incidence of successful spear phishing attacks out of all other APJ countries (82% vs 63% APJ average). And those attacks are rising fast—the rate was 28% higher than in 2022.

Compared to 14 countries worldwide, Japan had the highest number of users who say they never take a risky action (53% vs 29% global average). Japanese cultural values and its focus on discipline may play a role in this trend.

Security Responsibility



What risky actions are the worst? When security professionals and users are asked to rank them, there's clearly a disconnect. Users engage in four of the top five behaviours that security professionals in APJ rank as the riskiest. This may mean that users don't understand what's actually risky and what's not.

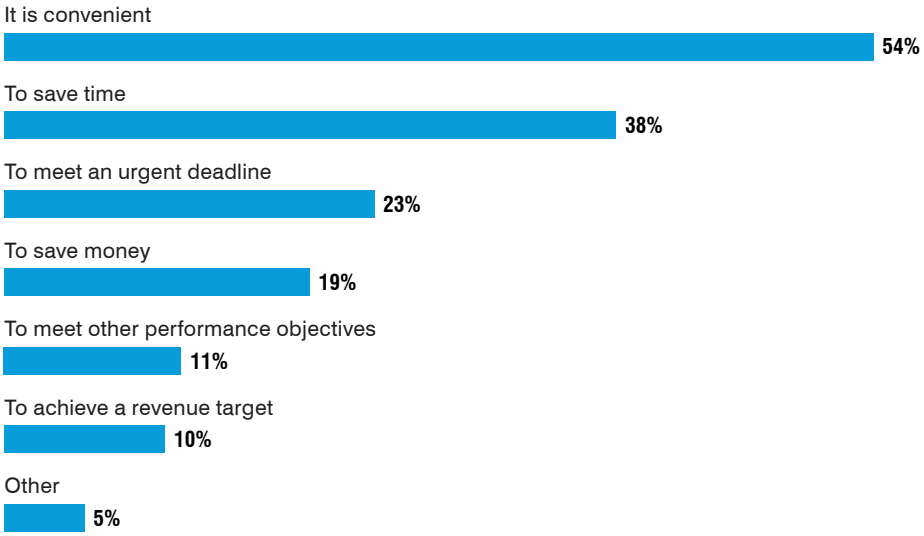
4 of 5

top risks cited by security pros are common behaviours among users

Rank	Risky Behaviour (Ranked by Sec Pros)	Risky Behaviour (Conducted by Users)
1	Access inappropriate website	Use work device for personal activities
2	Click on links or download attachments from someone I don't know	Reuse or share password
3	Respond to a message (email or SMS text) from someone I don't know	Connect without using VPN at a public place
4	Connect without using VPN at a public place	Access inappropriate website
5	Reuse or share password	Respond to a message (email or SMS text) from someone I don't know

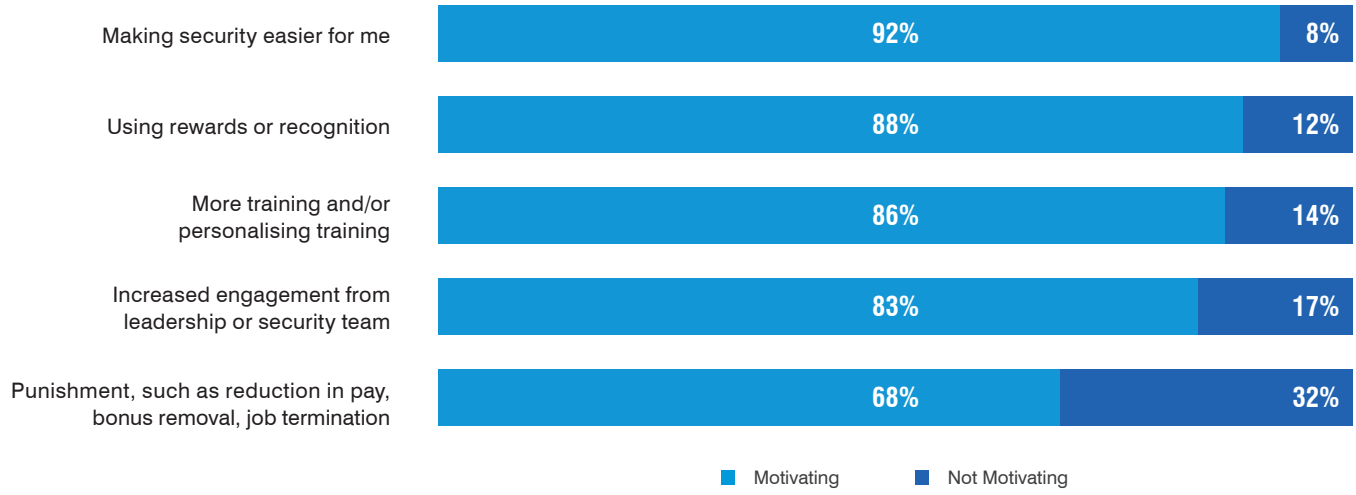
When it comes to why users in APJ take risky actions, the most common answer was "convenience" followed by "to save time." Notably, in Singapore users cited convenience more than anywhere else (64% vs 44% global average).

Why Users Take Risky Actions



APJ users are clear about why they take risky actions. But what would motivate them to prioritise security? As with our global results, the majority cited making security easier as the most effective motivator, and punishment as the least motivating.

Make Security a Priority for Users

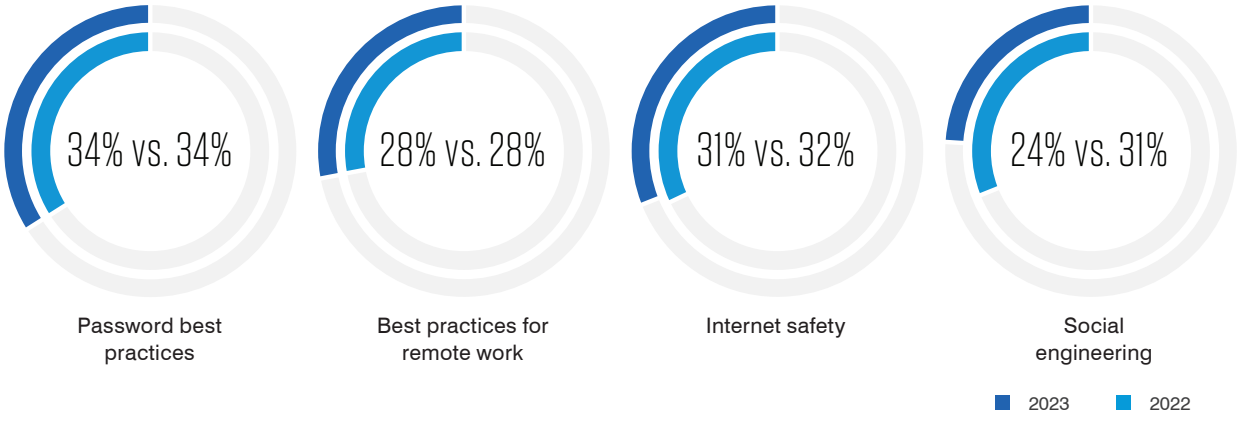


Opportunities for Improvement

APJ organisations use threat intelligence to inform their security awareness programs at the same rate as the global average (94%). But when it comes to using that intelligence, there are challenges. For example, business email compromise (BEC) is spreading rapidly across the region—at least 70% of respondents report being targeted. Yet only 18% of organisations in Singapore and 24% in South Korea train on the technique.

Another surprising finding—13% of Japanese organisations said that they do not use threat intelligence at all in their training. That's more than triple the global average of 4%. This might come down to the fact that security operations are often outsourced in Japan. And so threat intelligence is typically only used by those companies as well as a small group of government agencies and infrastructure firms.

When it comes to training users on critical security basics, APJ organisations are not changing much:



The one notable change was training on social engineering, which fell from 31% in 2022 to only 24% in 2023. This seems ill-advised given the proliferation of advanced social engineering attacks worldwide.

APJ Threat Landscape

Last year, the APJ threat landscape diverged from global trends in several key areas. Business email compromise fell overall, but non-English-speaking countries saw an increase. This could be linked to the rise of generative AI tools such as ChatGPT, which can be used to write convincing email lures in multiple languages. That likely explains why South Korea saw a sharp rise in these attacks with 76% of organisations being targeted, up from 58% in 2022.

70%

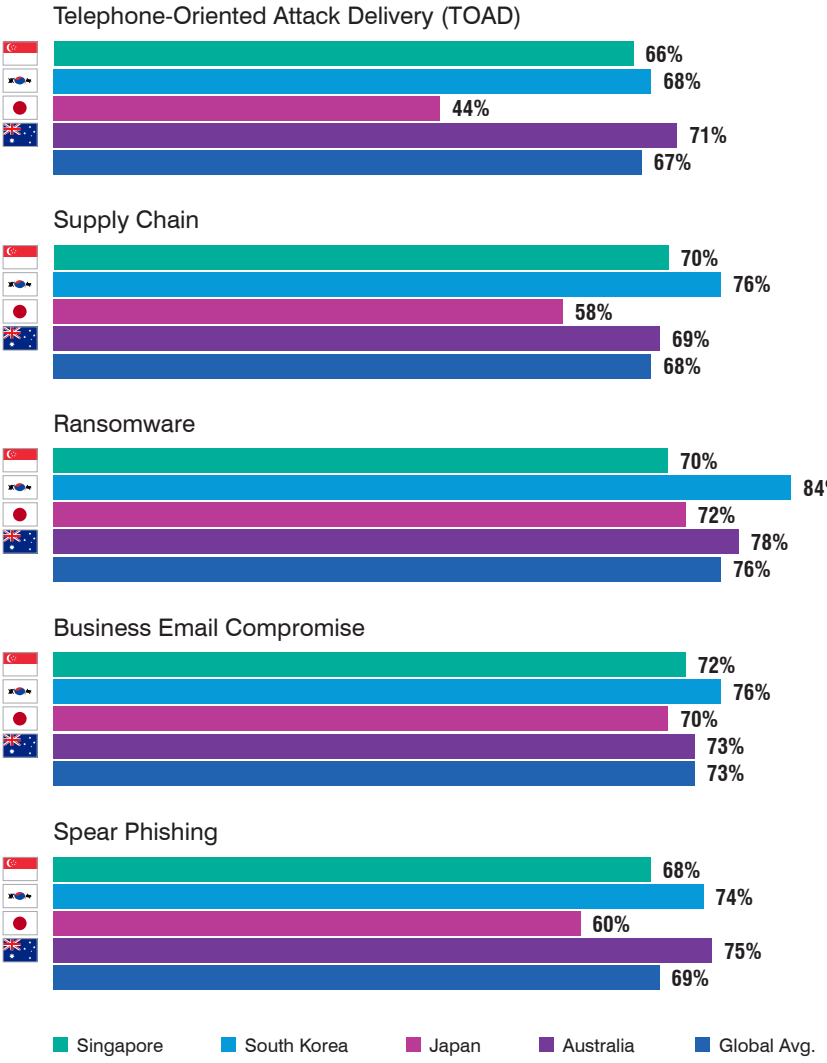
of Japanese organizations saw BEC attacks, a sharp increase from 58% the year before

Japan was also impacted by this trend. In the past, fraudulent emails were relatively easy to spot. But starting in early 2023 emails used new sophisticated grammar and formatting. At the same time, BEC attacks in Japan sharply increased, targeting 70% of organisations compared to 52% in 2022.

APJ organisations saw less telephone-oriented attack delivery attacks than the global average (62% vs 67%). In general, non-native English-speaking countries are less targeted by TOAD attacks as they often require threat actors to speak directly to their victims.

Australian organisations were targeted by spear phishing attacks at a higher rate than any other APJ country. However, in 2023 they saw a dramatic decrease in the number of successful attacks (56% vs. 88% in 2022). This might be due to an increase in user training on these attacks, which was 52% higher than in 2022.

Percentage Affected by Targeted Attacks



Ransomware

Ransomware remains a serious threat in APJ. Threat actors use email-based ransomware attacks more than any other email-based tactic in this region. On average, these attacks went up slightly in APJ—76% of organisations were targeted (vs 75% in 2022).

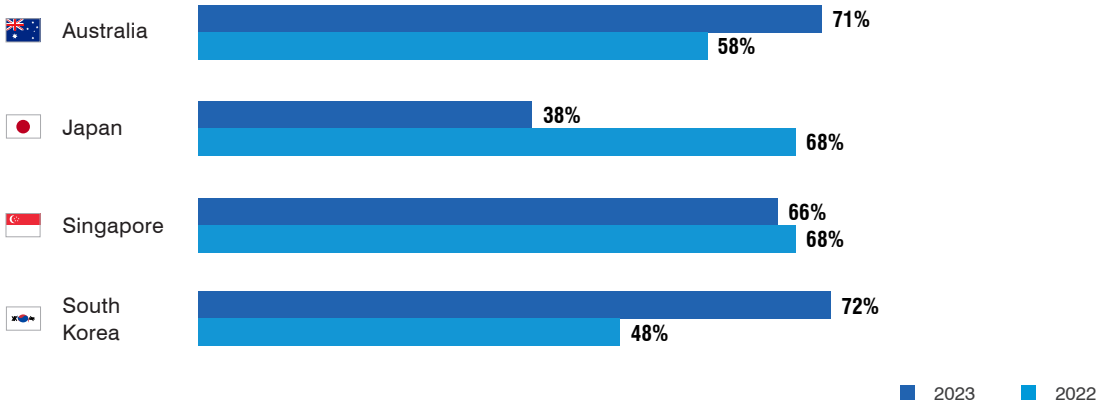
Ransomware Attack Trend

Ransomware infections also slightly increased from year to year across the APJ, from 61% in 2022 to 62% in 2023. This trend played out differently in each country, and there were several outliers.

South Korea, for example, saw a big swing from year to year. Ransomware infections jumped from 48% in 2022 to 72% in 2023. This is not surprising given that out of 120 countries that faced cyberattacks last year, South Korea was near the top of the list.

In contrast, ransomware infections in Japan plummeted (38% vs 68% in 2022). This might be partly due to its push over the past 12 months to adopt a defense-in-depth strategy.

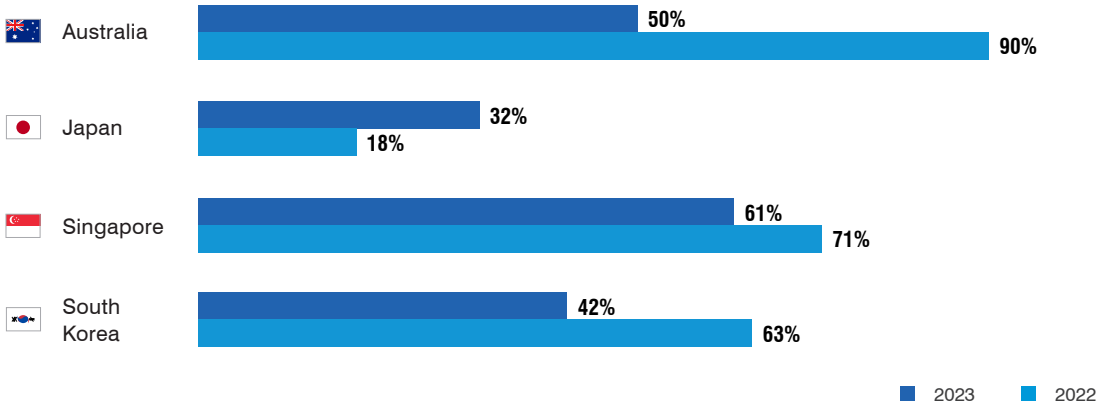
Ransomware Infection Trend



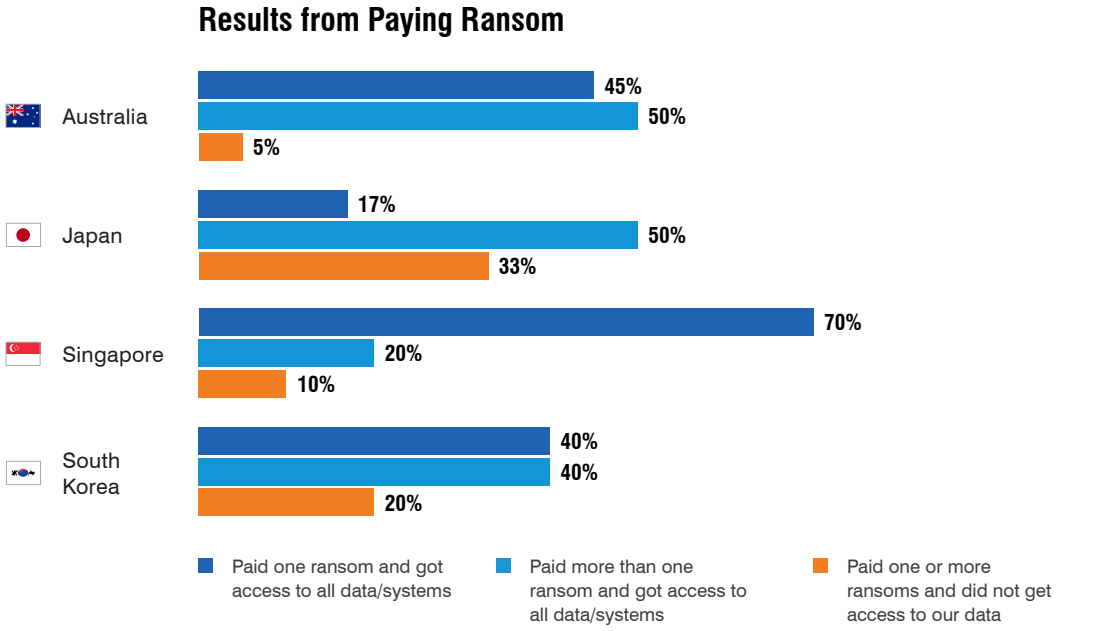
Notably, APJ countries are less willing to pay ransoms than other regions (46% vs 54% global average). That's down significantly from 2022 when the APJ average was 60%.

It's likely that policies and practices in Australia and Japan are contributing to this trend. While there's no law against paying a ransom in Australia, the federal government strongly discourages it, and blanket ban may not be far off. Whereas in Japan, there are already laws against supporting anti-social groups.

Percentage of Organisations that Paid a Ransom



Overall, ransom payments declined across the APJ at a significant rate. In Singapore, however, they were only down 10%. One potential reason for this might be that Singaporean organisations saw the most positive results when paying their first ransom with 70% receiving access to their data and systems. It helps that they are well-insured with 55% reporting their claim covered in full.



While paying the ransom may work well in Singapore, it also appears to make those organisations a target—27% of organisations experienced multiple ransomware attacks compared to the APJ average of 14%. This shows how threat actors do not stop exploiting organisations if they pay a ransom. In fact, it makes them more likely to come back.

South Korea seems to understand this equation. Although it has highest level of successful ransomware attacks in the APJ at 72%, more often than not threat actors go away empty-handed. Only 42% of South Korean organisations paid a ransom in 2023 (vs the 54% global average).

On a positive note, cyber insurance coverage levels have significantly improved over the past year. A full 90% of organisations across the region say that they are either fully or partially covered for ransomware attacks (vs 67% in 2022).

Recommendations

Our survey shows that users understand their behavior carries risk. But this often isn't enough to convince them to prioritise security. This might be for the sake of convenience, or to save time, or because they simply don't know if IT security is their responsibility.

Unfortunately, cybercriminals are taking full advantage of this confusion. But there are a few approaches that can make an immediate difference in changing user behaviour and reducing risk:

For users who already understand that security is their responsibility

Provide tools that empower people to be more proactive. Email reporting buttons make it simple to report suspicious messages. And "nudging" technologies such as email warning tags can prompt users to act. Also consider building a champions network and reward system to encourage these users to model best practice and advocate for others who are unsure of what to do.

For users who are unsure or don't believe that security is their responsibility

Make education personal and relevant to individual roles and responsibilities. Increase communication from business and security leaders to better inform users of their responsibilities and their impact on the organization.

It's also important to provide best-in-class security education, prevention, detection and response. Advanced solutions can help balance stricter security controls with productivity by reducing the number of threats faced by users. For example, deploying an email security solution that is 99.9% effective means that most users will never have to decide how to respond to a suspicious link.

Finally, work with business stakeholders and prioritise ease-of-use when implementing security policies. Users will be less inclined to circumvent systems if security aligns with their goals. And they are more likely to use a control if it is intuitive and does not require any training.

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.

0402-018-01-01