ARMIS

THE STATE OF CYBERWARFARE

ARMIS STATE OF CYBERWARFARE AND TRENDS REPORT: 2022-2023

REGIONAL ANALYSIS

APJ

(AUSTRALIA, JAPAN, SINGAPORE)

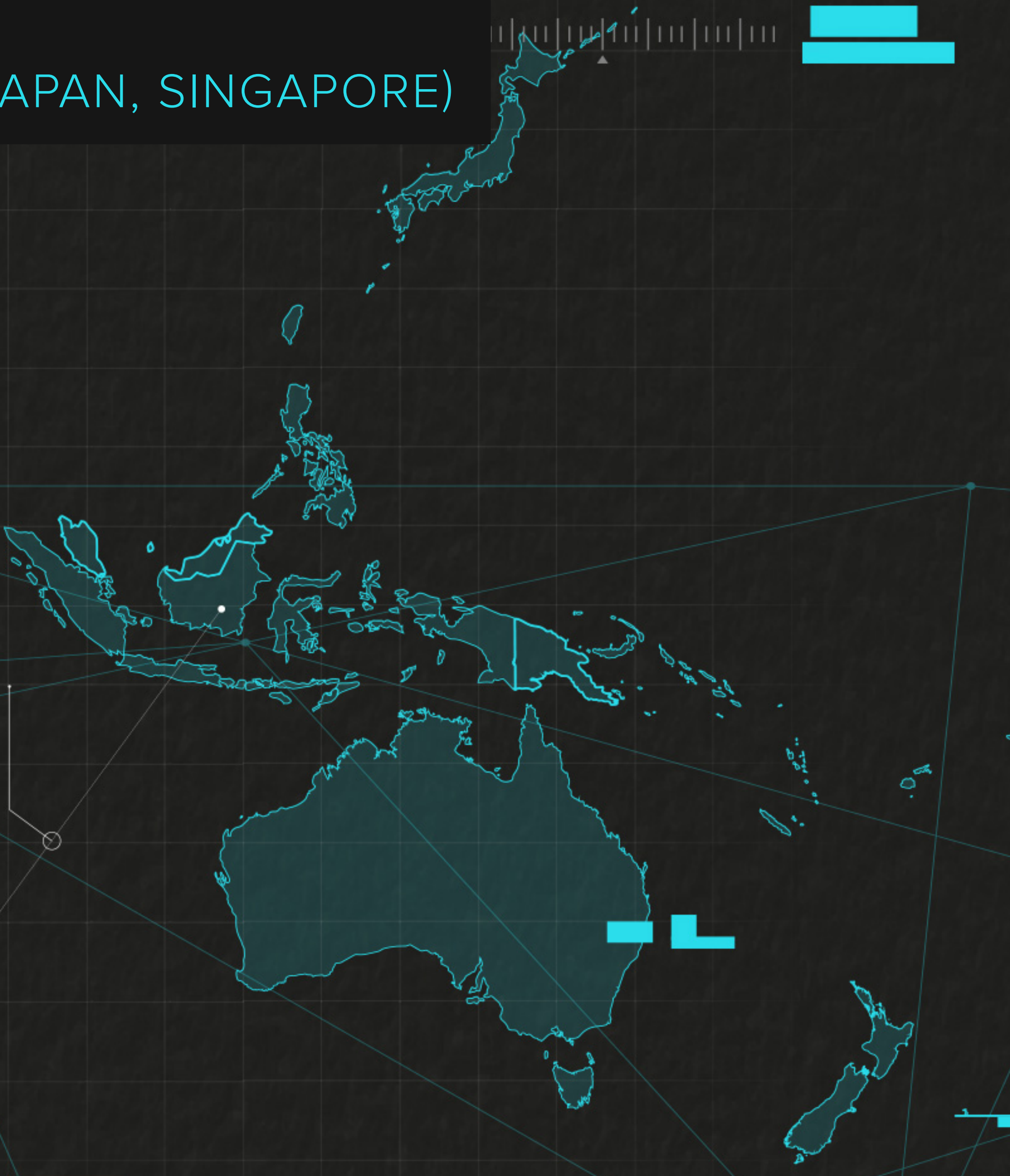


TABLE OF CONTENTS

INTRODUCTION

If you've reviewed the global Armis State of Cyberwarfare and Trends Report: 2022-2023, you know that it's critical for business and IT leaders to understand the evolving threat landscape surrounding cyberwarfare, so that they can improve their cybersecurity posture to defend against these attacks. To prepare this report, Armis commissioned a study surveying 6,021 IT and security professionals globally to determine worldwide trends as they relate to security professionals' sentiments on cyberwarfare, attack patterns, cyber spending, and more. Responses were gathered between September 22, 2022 and October 5, 2022.

Armis utilized data from its award-winning Asset Intelligence and Security Platform to verify the survey results against real-world data trends. Proprietary data from the Armis platform collected June 1, 2022 through November 30, 2022 confirmed that cyberattacks haven't slowed, only worsened. Threat activity against the global Armis customer base increased by 15% from September to November when compared to the three months prior. Further, Armis identified the largest percentage of threat activity against critical infrastructure organizations, with healthcare organizations the second most targeted when compared to various industries.

In addition to these global findings, Armis has prepared regional findings and country-by-country analysis to offer unique, localized insights which may be more impactful for individual readers depending on where they are physically based and the countries in which their business operates. **For this country-by-country analysis, we will zoom in on the findings pulled from the 1,513 respondents who shared insights for our survey that are based out of Australia (511), Singapore (501), and Japan (501) and work across industries including healthcare, manufacturing, retail, financial services, and more.**

ARMIS.
SECURE VULNERABLE ASSETS
FOCUS ON HIGH-RISK VULNERABILITIES THAT CAN CAUSE COSTLY DISRUPTIONS
LEARN MORE

SUMMARY OF FINDINGS

Overall, Armis identified a number of key differences and trends when analyzing responses from IT and security professionals from the three APJ countries surveyed (Australia, Japan, and Singapore) when compared to other global respondents from companies across EMEA and the U.S. Below, we dive deeper into those findings and the trends they're indicative of.

At a high level across the region, threat levels are on the rise. However, the number of breaches among companies we surveyed in APJ remains low when compared to those located in other regions globally, particularly EMEA-based organizations. With this, a portion of respondents from APJ have indicated they're unconcerned or indifferent about the impact of cyberwarfare on various aspects of their organizations. Although they clearly have been more successful than others when thwarting these attacks, when grouped, these organizations are only demonstrating an average level of preparedness when compared to other respondents globally.

When diving deeper into a country-by-country analysis, respondents from Australia, Japan, and Singapore each indicated different trends happening locally:

- Australians are concerned about the threat of cyberwarfare and are making business decisions in response to these threats. They're also exhibiting high confidence in their government's ability to defend against cyberwarfare, despite the recent string of cyberattacks that have had far-reaching impacts on millions of Australians.
- In Japan, respondents overall are showing concern for cyberwarfare, but an alarming number are still indifferent to these threats. One standout finding when comparing Japan to respondents from other countries? They're the least likely to pay in the event of a ransomware attack.
- Singapore respondents - known for being tech-forward and innovative – have shared they're stalling or stopping digital transformation projects due to the threat of cyberwarfare. This increased threat activity will result in them continuing to invest in improving their cybersecurity posture in the months ahead.

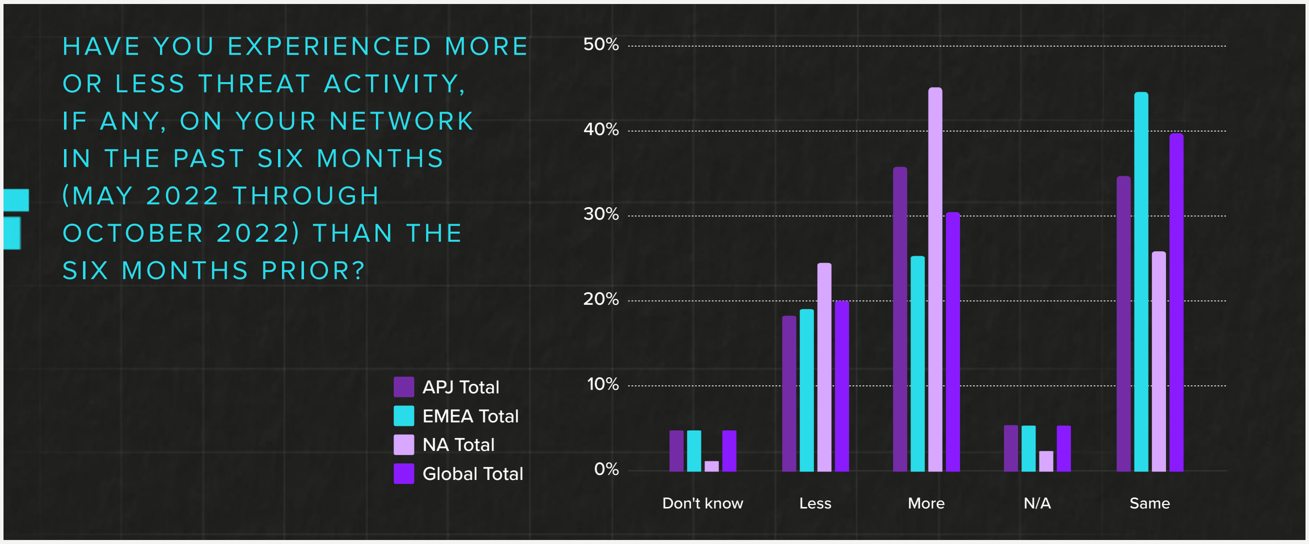
Continue reading for more detail on these and other findings.

REGIONAL ANALYSIS APJ (AUSTRALIA, JAPAN, SINGAPORE)

THREATS REGIONALLY ARE ON THE RISE, ALTHOUGH BREACHES REMAIN LOW COMPARATIVELY ACROSS THE GLOBE

According to the findings of this survey, respondents from the three APJ countries surveyed (Australia, Japan, and Singapore) have experienced the least number of cybersecurity breaches when compared to global respondents, with 53% of IT and security pros based in Australia, Japan, and Singapore indicating their company has experienced one or more cybersecurity breaches. When zooming in further, Singapore has experienced the most cybersecurity breaches, with 60% indicating their organization has been breached once or more. Fifty-seven percent of Australian respondents and 44% of Japanese respondents have experienced one or more breaches. Comparatively, almost 3 in 5 (58%) respondents in EMEA and 7 in 10 (73%) U.S. respondents indicated that their organizations experienced one or more cybersecurity breaches.

While the respondents we surveyed across the APJ region experienced fewer breaches when compared to EMEA respondents, there is a higher percentage of IT and security pros in Australia, Japan, and Singapore experiencing increased threat activity on their networks. Between May 2022 and October 2022, these respondents indicated a 36% increase in threat activity on their networks when compared to the six months prior. When asked the same question, only 25% of respondents in EMEA answered the same. Moreover, around 3 in 5 (61%) of respondents from the APJ countries we surveyed have had to report an act of cyberwarfare to authorities, compared to just 33% in EMEA.

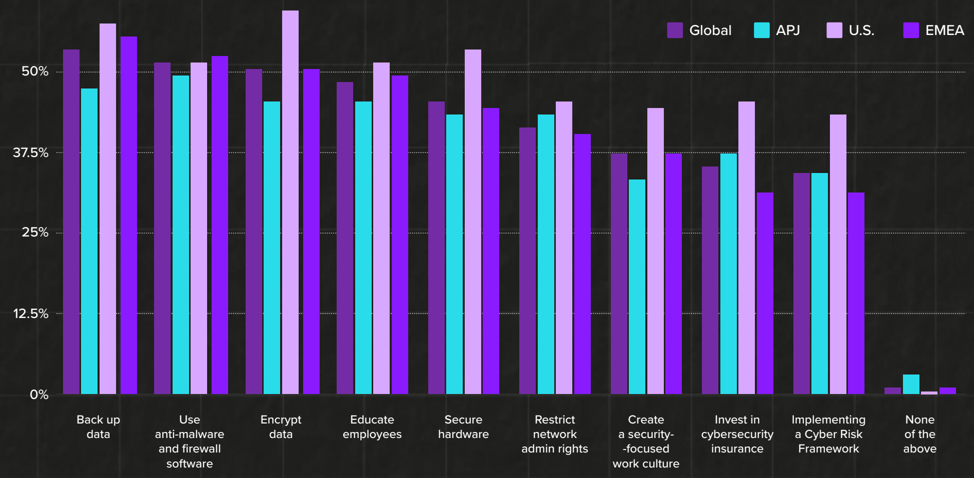

HAVE YOU EXPERIENCED MORE OR LESS THREAT ACTIVITY, IF ANY, ON YOUR NETWORK IN THE PAST SIX MONTHS (MAY 2022 THROUGH OCTOBER 2022) THAN THE SIX MONTHS PRIOR?

This survey also found threat activity on Australia, Japan, and Singapore-based businesses is having an impact as decisions are being made across these organizations. Over 3 in 5 (58%) IT professionals surveyed indicated that their organization has stalled or stopped digital transformation projects due to the threat of cyberwarfare. Further, almost 3 in 5 (59%) say the threat of cyberwarfare will slow digitization.

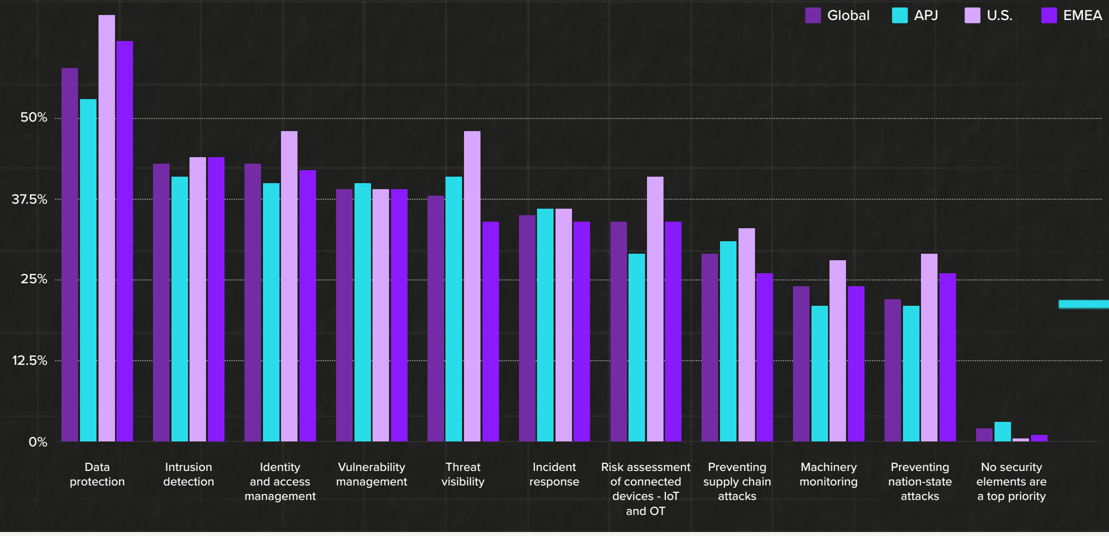
THE CYBERSECURITY PRACTICES OF APJ COMPANIES SURVEYED THAT ARE IMPLEMENTED AND PRIORITIZED ARE ON PAR WITH THE GLOBAL AVERAGE

Despite this threat level and potential impacts on businesses, well over a quarter (29%) of IT professionals surveyed are unconcerned or indifferent about the impact of cyberwarfare on their organization as a whole and 3 in 10 (30%) are unconcerned or indifferent about the impact of cyberwarfare on their company's critical infrastructure or their company's services. This lack of concern could be due to the fact that respondents overall have implemented security measures on par with global averages and are prioritizing certain security elements more consistently when compared to respondents from EMEA and the U.S. They have also been more successful in thwarting cyberattacks to date.

WHICH OF THE FOLLOWING CYBERSECURITY PRACTICES, IF ANY, IS IMPLEMENTED INTO YOUR COMPANY/ORGANIZATION?



WHICH SECURITY ELEMENTS, IF ANY, ARE A TOP PRIORITY?



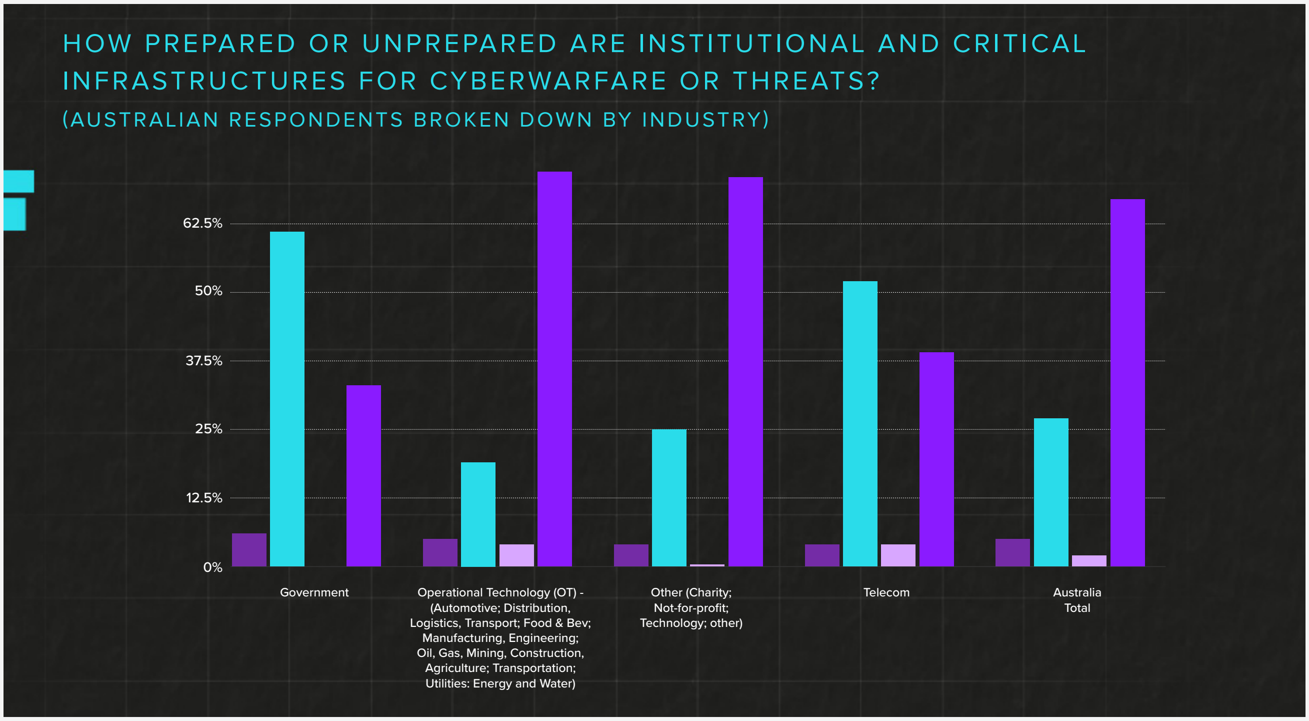
Next, we'll take a closer look at a country-by-country analysis of trends.

COUNTRY-BY-COUNTRY ANALYSIS AUSTRALIA TRENDS FROM THE ARMIS STATE OF CYBERWARFARE AND TRENDS REPORT: 2022-2023

CONCERNS ABOUT THE THREAT OF CYBERWARFARE ARE IMPACTING BUSINESS DECISIONS IN AUSTRALIA

Australian respondents are seeing more threat activity than the global average (31%). Forty percent of Australian respondents experienced more threat activity on their networks between May and October 2022 when compared to the six months prior and over half (57%) have experienced a cybersecurity breach at their organization.

In regard to cyberwarfare specifically, over two-thirds (68%) of Australian respondents have had to report an act of cyberwarfare to the authorities. This could help to explain why 83% of Australian IT and security professionals are concerned about the impact of cyberwarfare on their company as a whole, while 84% are concerned about their company's critical infrastructure and 83% are concerned about their company's services. Despite these concerns, the vast majority (93%) of the Australian industry leaders surveyed feel confident in the preparedness of institutional and critical infrastructures to respond to these threats.


HOW PREPARED OR UNPREPARED ARE INSTITUTIONAL AND CRITICAL INFRASTRUCTURES FOR CYBERWARFARE OR THREATS?
(AUSTRALIAN RESPONDENTS BROKEN DOWN BY INDUSTRY)

The threat of cyberwarfare goes beyond these concerns and is driving business decisions. A majority of Australian respondents (79%) stated that they have stalled or stopped digital transformation projects due to the threat of cyberwarfare. And, 66% say they are reconsidering suppliers as a result of the Russia-Ukraine conflict - more than the average across the APJ countries we surveyed (54%) and also more than the global average (51%).

AUSTRALIANS ARE VERY CONFIDENT IN THEIR GOVERNMENT'S ABILITY TO DEFEND AGAINST CYBERWARFARE DESPITE THE STRING OF RECENT, HIGH-IMPACT BREACHES

According to this survey, 92% of Australian respondents are confident that their government can defend against cyberwarfare, compared to the global average of 71%. Australian respondents also overwhelmingly agree (95%) that guidance from their government, such as the recommendations known as The Essential Eight, is mandatory.

Despite this confidence, eight local companies, including Medibank Private and Optus, were breached between September 2022 and mid-November 2022.

The Medibank breach alone impacted 10 million current and former customers. Government agencies are now stepping in following these attacks in the hopes of limiting the impact. The Attorney General's investigations have implicated a criminal gang located in Russia, and the Australian government has increased the fines imposed on companies for data breaches happening in Australia. As a result of the public outcry from both Medibank and Optus, it's likely that wider reforms of Australia's privacy laws will follow, including greater powers for the Office of the Australian Information Commissioner, the privacy watchdog. This has led to a peak in demand for cybersecurity like never before. Australian respondents demonstrated the highest level of support for conscription into a cyber defense league if their country is drawn into a cyberwar conflict (70%) when compared to the global average (63%) and the survey's regional APJ average (59%).

ARMIS®
www.armis.com
THREAT DETECTION & RESPONSE
ENSURE ASSETS ARE SECURED. ALWAYS. EVERYWHERE.
WATCH THE VIDEO

COUNTRY-BY-COUNTRY ANALYSIS JAPAN TRENDS FROM THE ARMIS STATE OF CYBERWARFARE AND TRENDS REPORT: 2022-2023

IT AND SECURITY PROS IN JAPAN ARE CONCERNED ABOUT CYBERWARFARE, BUT MANY ARE SEEMINGLY INDIFFERENT TO THE THREATS

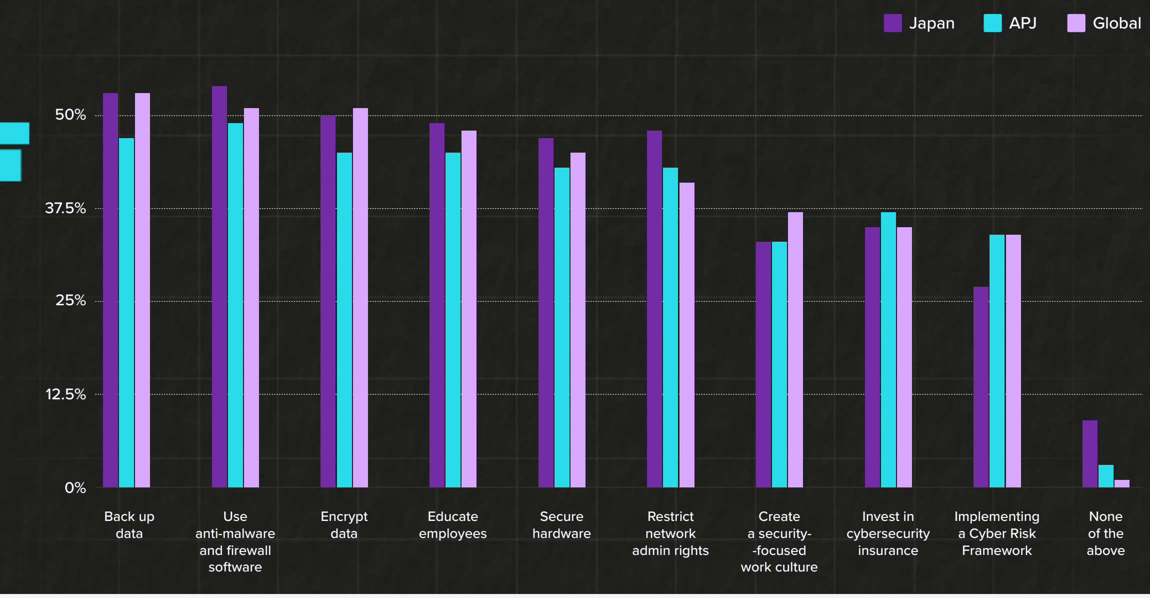
Forty-four percent of respondents from Japan have experienced a cybersecurity breach at their company. And, just over 7 in 10 (71%) of IT professionals surveyed think international political conflicts and national breaches, such as the situations in Ukraine and Taiwan, will have an impact on their company's cybersecurity. On top of this, Japanese respondents exhibited significantly less confidence (33%) in their government's ability to defend against cyberwarfare when compared to the others we surveyed in APJ and globally, where the average confidence level was 71%.

When asked about the impact of cyberwarfare on different aspects of their work, 59% of respondents are concerned about their organization as a whole, while 58% are concerned about their company's critical infrastructure, and 56% expressed concern for their company's services. Sixty percent of Japanese respondents said their organization has programs and practices currently in place specifically designed to respond to cyberwarfare threats, significantly less than the APJ respondent average (79%) and the global average (84%).

Despite this, respondents from Japan feel their companies have sufficient budget for cybersecurity programs, people, and processes, with 62% of respondents somewhat agreeing or strongly agreeing with that statement. However, when asked about security elements that are a top priority to their organization, 9% selected "no security elements are a top priority." Another 9% of Japanese respondents said they had not implemented any standard cybersecurity practices, such as data backup, data encryption, and the creation of a cybersecurity-focused work culture. That being said, the remainder of respondents demonstrated an above-average level of preparedness when compared to the APJ and global averages.

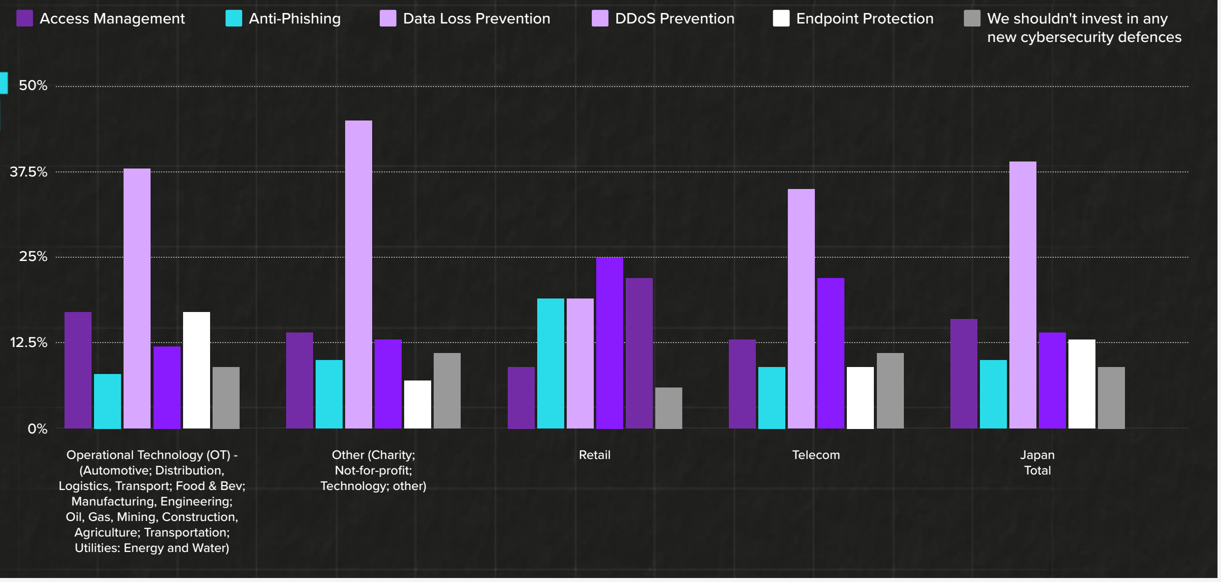
ARMIS
ADVANCED VULNERABILITY MANAGEMENT
ASSESS THE RISK ASSOCIATED WITH EVERY ASSET AND PRIORITIZE REMEDIATING CRITICAL VULNERABILITIES.
LEARN MORE

WHICH OF THE FOLLOWING CYBERSECURITY PRACTICES, IF ANY, IS IMPLEMENTED INTO YOUR COMPANY/ORGANIZATION?



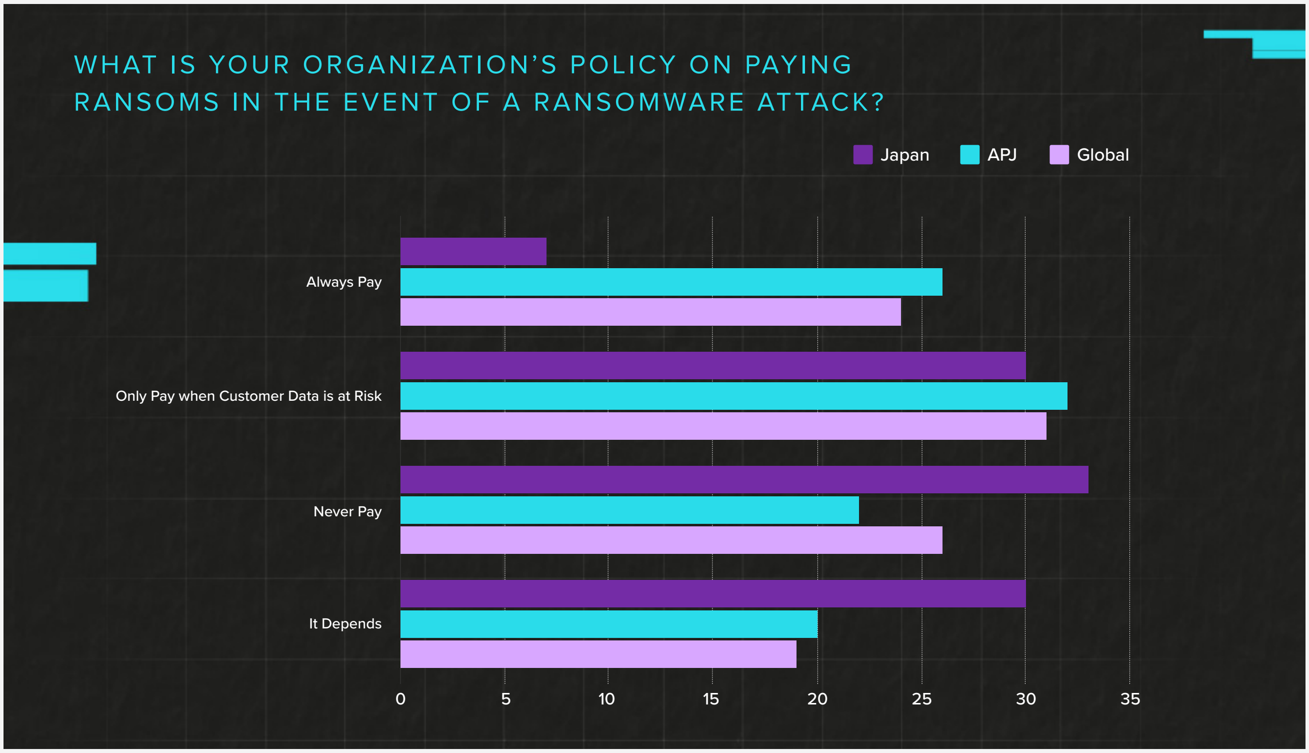
With the new economic security bill in Japan aimed towards protecting critical infrastructure and supply chains from further attacks, respondents indicated their organization's main priorities should be to invest further in data loss prevention (39%), followed by access management (16%), DDoS prevention (14%), and endpoint protection (13%). Nine percent of respondents indicated they believe that their organizations should not invest in any new cybersecurity defences.

WITH THE NEW ECONOMIC SECURITY BILL IN JAPAN TO PROTECT CRITICAL INFRASTRUCTURE AND SUPPLY CHAINS FROM CYBER ATTACKS, WHAT, IF ANYTHING, ARE SOME OF THE CYBERSECURITY DEFENCES YOUR ORGANIZATION SHOULD FURTHER INVEST IN?



JAPANESE COMPANIES ARE THE LEAST LIKELY TO PAY IN THE EVENT OF A RANSOMWARE ATTACK

When asked about their organizations' policies on paying ransoms in the event of a ransomware attack, respondents from Japan indicated they would be the least likely globally to pay in the event an attack occurred.


WHAT IS YOUR ORGANIZATION'S POLICY ON PAYING RANSOMS IN THE EVENT OF A RANSOMWARE ATTACK?

COUNTRY-BY-COUNTRY ANALYSIS SINGAPORE TRENDS FROM THE ARMIS STATE OF CYBERWARFARE AND TRENDS REPORT: 2022-2023

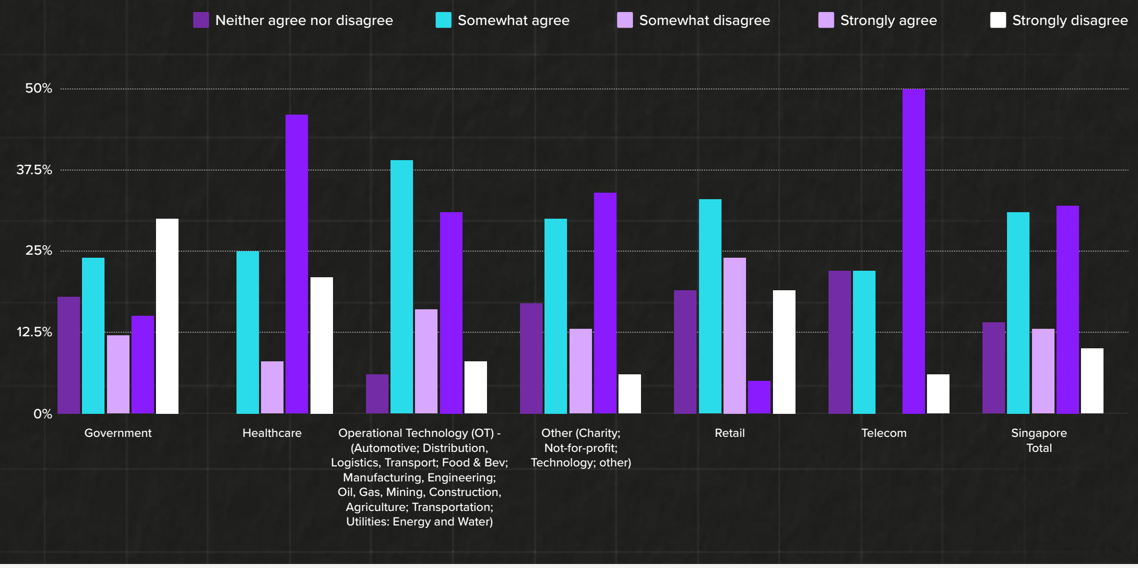
RESPONDENTS ARE STALLING DIGITAL TRANSFORMATION PROJECTS DUE TO THE THREAT OF CYBERWARFARE

Singapore is known globally for being a technology and innovation hub. However, these findings from Armis strongly suggest that the threat of cyberattacks is posing a separate threat to the city state's development ambitions. In response to the threat of cyberwarfare, 63% of local respondents indicated their organization has stalled or stopped digital transformation projects – significantly higher than both the survey's APJ average (58%) and the global average (55%).

With the new economic security bill in Japan aimed towards protecting critical infrastructure and supply chains from further attacks, respondents indicated their organization's main priorities should be to invest further in data loss prevention (39%), followed by access management (16%), DDoS prevention (14%), and endpoint protection (13%). Nine percent of respondents indicated they believe that their organizations should not invest in any new cybersecurity defences.

TO WHAT EXTENT DO YOU AGREE OR DISAGREE WITH THE FOLLOWING STATEMENTS ABOUT YOUR ORGANIZATION'S CYBER SECURITY PROCESSES:

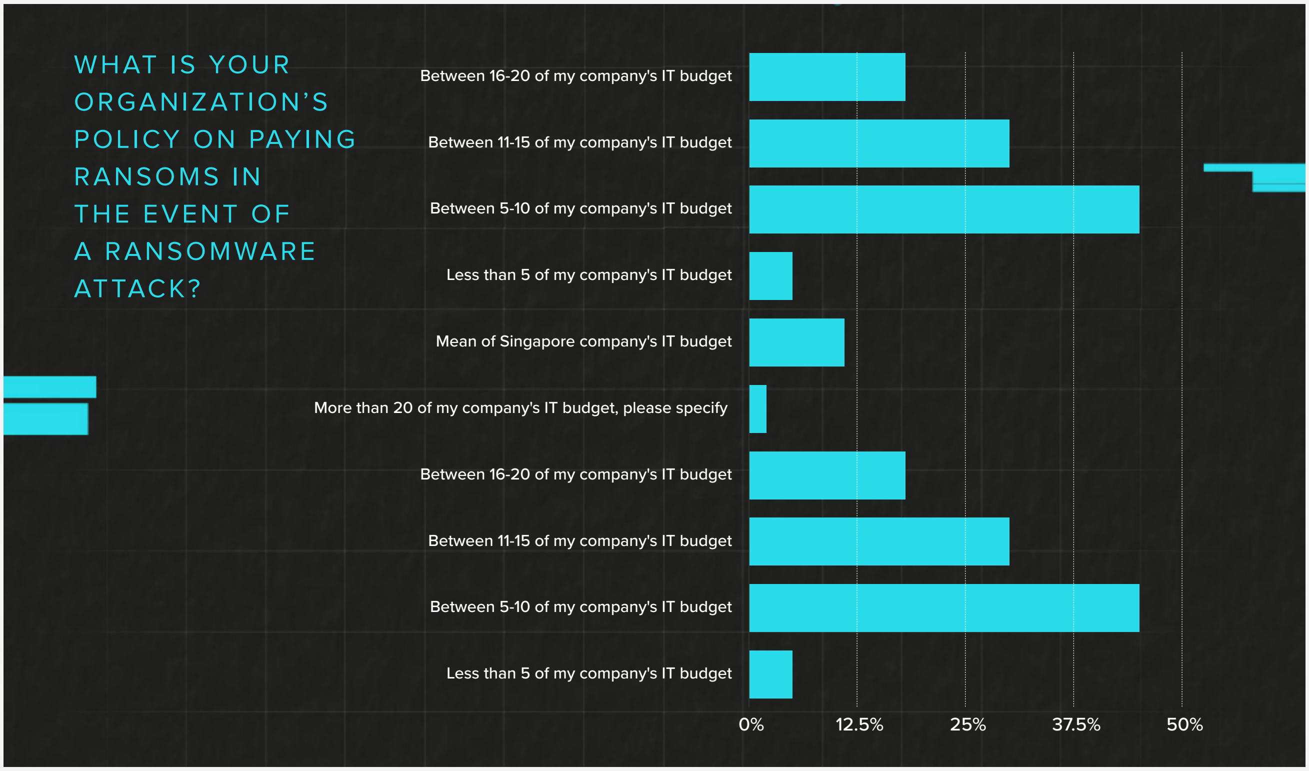
"MY ORGANIZATION HAS STALLED OR STOPPED DIGITAL TRANSFORMATION PROJECTS DUE TO THE THREAT OF CYBERWARFARE."



INCREASED THREAT ACTIVITY WILL RESULT IN HIGHER SECURITY SPENDING

Three in five (60%) IT and security professionals surveyed in Singapore have experienced a cybersecurity breach at their company. And, 36% of local respondents indicated they've experienced more threat activity on their networks between May and October 2022 when compared to the six months prior. Healthcare respondents (63%) have seen the highest increase in threat activity when looking at the same timeframe, followed by those from telecommunications firms (53%).

A large majority of Singapore respondents (83%) believe their companies have allocated sufficient budget for cyber security programs, people, and processes, and 89% feel their organizations are prepared with a comprehensive cyber defence program. Between May and October 2022, Singapore respondents invested in a number of cybersecurity tools and services. The most popular areas of investment included endpoint protection (46%), security information and event management (SIEM) (44%), access management (43%), vulnerability management (43%), and managed security service providers (MSSPs) (40%). Eighty-three percent of IT and security pros think it's likely that in response to recent and ongoing, sudden global events (such as the pandemic, Ukraine war, etc.), their companies will invest more of their budgets into cybersecurity.



WHY DO THESE FINDINGS MATTER?

In the wake of a shifting threat landscape, businesses have a long way to go when it comes to being fully prepared for the threat of cyberwarfare. As defenses grow stronger, so do attackers, and businesses need to ensure they are taking the proper steps to adapt now. The cyberwarfare threat is halting technological advancement from the implementation of digital transformation projects. A proactive approach to security which includes developing a proper plan with complete asset visibility that is tested regularly is a step in the right direction for businesses as they work to protect against this growing threat.

WHAT CAN YOUR ORGANIZATION DO TO PROTECT ITSELF?

So, what can organizations do? Early detection and continuous monitoring is the best way to improve the security posture and remediate quickly. After all, if you don't know you have a problem, you can't fix it. Similarly, if you can't see an asset, you can't protect it. This is where Armis can assist.

ARMIS ASSET INTELLIGENCE PLATFORM

The **Armis Asset Intelligence Platform** provides unified asset visibility and security across all asset types, including information technology (IT), internet of things (IoT), operational technology (OT), internet of medical things (IoMT), cloud, and cellular-IoT — both managed and unmanaged. Delivered as an agentless software-as-a-service (SaaS) platform, Armis seamlessly integrates with existing IT and security stacks to quickly deliver the contextual intelligence needed for improving an organization's security posture, without disrupting current operations or workflows. Armis helps customers protect against unseen operational and cyber risks, increase efficiencies, optimize the use of resources, and safely innovate with new technologies to grow their business – no matter the threat, cyberwarfare or other.

Register today for a Security Risk Assessment to learn which assets are most vulnerable to attack. Use these insights to prioritize your risk mitigation strategy and ensure full compliance with regulatory frameworks that require you to identify and prioritize all vulnerabilities.

To request a custom demo from Armis, please visit: armis.com/demo.

To dive deeper into the findings of the Armis State of Cyberwarfare and Trends Report: 2022-2023 on a global scale, please visit: **armis.com/cyberwarfare.**

THE STATE OF CYBERWARFARE

ABOUT ARMIS

Armis, the leading asset visibility and security company, provides the industry's first unified asset intelligence platform designed to address the new extended attack surface that connected assets create. Fortune 100 companies trust our real-time and continuous protection to see with full context all managed, unmanaged assets across IT, cloud, IoT devices, medical devices (IoMT), operational technology (OT), industrial control systems (ICS), and 5G. Armis provides passive cyber asset management, risk management, and automated enforcement. Armis is a privately held company and headquartered in California.

armis.com

info@armis.com

20230110-1