CrowdStrike Products

CROWDSTRIKE

ASIA PACIFIC AND JAPAN (APJ)

STATE OF CYBERSECURITY SURVEY

Taking the pulse of business leaders on cybersecurity in the wake of the COVID-19 pandemic

INTRODUCTION

The first half of 2020 brought unprecedented disruption, change and the need for adaptation to businesses and organizations across the world. While leaders have moved to identify and confront a slew of challenges, cybersecurity adversaries have acted just as quickly to take advantage of uncertainty and changing dynamics.

Sharing knowledge, experiences and insights has always been integral to effective cybersecurity protection. Knowing what organizations are experiencing — both in terms of adversaries and their activity, and also internally, as processes, technologies, budgets and opinions shift — is fundamental to achieving widespread best practices.

The CrowdStrike® Asia Pacific and Japan (APJ) State of Cybersecurity survey asked over 2,000 business leaders in Australia, Hong Kong, India, Indonesia, Japan, Malaysia, New Zealand, Philippines, Singapore and Thailand about their cybersecurity practices during the COVID-19 pandemic, and their future plans as the world enters a period of tentative revival.

By identifying and sharing the gaps, needs and intentions of some of APJ's senior business leaders, organizations can work to ensure that cybersecurity is not a cause of business failure in the challenging times ahead.

Sharing knowledge, experiences and insights has always been integral to effective cybersecurity protection.

RESPONSE NOW NEEDS TO MATCH INCREASED RISK DURING COVID-19

Throughout the COVID-19 pandemic, CrowdStrike Intelligence has observed an increase in malicious activity. While the scope and variety of these attacks have been significant, there are some common themes.

- **COVID-19 eCrime:** eCrime adversaries have used social engineering techniques and malicious documents referencing COVID-19 to prey on the public's fear, often using subjects such as health guidance, containment and infection-rate news to mount successful attacks.

- **Targeting of Remote Services:** Many organizations have expanded the use of software as a service (SaaS) and cloud-based remote connectivity services in order to enable and support employees working from home. Criminal actors continually seek to collect credentials for these services, potentially allowing them to gain access to these SaaS accounts and the victim organization's data. The eCrime big game hunting (BGH) ransomware industry in particular leverages Remote Desktop Protocol (RDP) brute forcing or password spraying for initial entry.

- **Vishing Robocall and Tech Support Scams:** As employees shift to flexible work arrangements such as telecommuting, they will increasingly rely on phone communications to maintain and continue business operations. Adversaries have been observed taking advantage of this situation to conduct malicious operations attempting to mimic official business communications.

As the pandemic spread, changes and challenges piled up for business leaders across APJ, and cybersecurity slipped down the list of priorities. This is evidenced by the fact that almost four in ten organizations haven't changed their security programs since the beginning of the pandemic, opening their organizations to new and more sophisticated attacks.

Foremost among the advice CrowdStrike has given businesses during the pandemic is to ensure employees at all levels and in every department become and remain aware of potential cyber threats, and how they have changed since the emergence of COVID-19. However, only 61% of business leaders have received warnings about COVID-19-themed malware, with 36% not receiving any warnings, and almost four in ten not receiving additional training in security. For those respondents who had a cybersecurity emergency response plan, 27% haven't changed that plan as a result of COVID-19. This leaves organizations vulnerable to a lack of knowledge and planning should a breach occur.

These gaps in knowledge, planning and training are understandable given the fundamental changes that have occurred. However, they now need to be closed quickly. There are signs that business leaders recognize this, with 76% planning more security training in the future as a result of the pandemic and its associated risks.

Employees at all levels and in every department must become and remain aware of potential cyber threats, and how they have changed since the emergence of COVID-19.

CHANGING SUPPLY CHAINS OPEN UP NEW CYBER RISKS

Fifty-eight percent of business leaders say their supply chain has changed since COVID-19 began, which can be attributed to the COVID-19 lockdowns. While 70% of business leaders acknowledge the supply chain is a potential cyber threat, almost one in five respondents who had seen a change in the supply chain have not conducted an audit of cybersecurity in that supply chain, meaning new vulnerabilities are not only present, but leaders also do not have adequate visibility over them.

Shifts that occurred in record time out of necessity will need to be made permanent, requiring more change and risk.

FROM PANIC AND PANDEMIC TO POTENTIAL AND PROTECTION

That the world has changed, considerably and permanently, is beyond question.

The way organizations now operate is no exception to this rule. Forty-four percent of business leaders report COVID-19 has accelerated their move to cloud solutions, 82% say it changed the way they interact or deliver products and services to customers and 82% expect to continue having staff working from home or move to a hybrid model.

Business leaders are now increasingly turning their thoughts to recovery and revival but acknowledge the bumpy road ahead. While 72% say economic conditions and 70% say new waves of COVID-19 are main threats in the latter half of 2020, cybersecurity follows close behind with 56%.

This concern is understandable. Organizations will continue to change and update systems and devices, while issues around access and use of data come to the fore. Shifts that occurred in record time out of necessity will need to be made permanent, requiring more change and risk.

Respondents stated that the top cybersecurity challenges in the next 18 months are a remote workforce (54%), new regulations (49%) and the costs associated with compliance (48%), followed closely by limited budgets (47%) and difficulty training staff (41%).

Remote working has dominated much of the economic conversation during the first half of 2020, and there is no sign of that ending. Not only is it the top cybersecurity challenge, 51% of business leaders think it will put them personally at more risk of a cyberattack and 65% believe it will put their companies more at risk.

CrowdStrike suggests the following key factors should be part of every organization's security strategy to help overcome the threats of remote working:

- Make sure your current cybersecurity policy includes remote working
- Plan for BYOD (bring your own device) devices connecting to your organization
- Be aware that sensitive data may be accessed through unsafe Wi-Fi networks
- Ensure cybersecurity hygiene and visibility
- Provide employees continued education on threats
- Ensure crisis management and incident response plans are executable by a remote workforce

Limited budgets are likely to be a frequent factor in business decision-making in the months and years to come, but 65% of business leaders expect technology budgets to increase, even with recessionary pressures on many other parts of the business.

Encouragingly, among those respondents who believe there should be more investment in remote working, the highest number (74%) list enhancement of cybersecurity measures as a priority for additional investment, 69% list the enhancement of the network environment and 59% list the business process optimization.

Remote working has dominated much of the economic conversation during the first half of 2020, and there is no sign of that ending.

RECOMMENDATIONS

EDUCATE

The human element of cybersecurity is vital, particularly in an environment where employees are using their own devices in their own homes or other locations. Businesses must ensure that every member of the staff is aware of the threats posed, how these threats are changing and how to best combat them. Through CrowdStrike University, IT and security staff can receive professional training and education services ranging from introductory to advanced subject matter, including courses designed for senior business leaders.

CrowdStrike maintains a **remote workforce cybersecurity hub**, which is a useful resource to help understand the evolving threat landscape and the techniques organizations all over the world are using to deal with these enormous changes.

PREPARE

As the results of the survey show, remote or hybrid working is here to stay. Organizations need to prepare for this by creating plans, response scenarios and simulations that reflect it. Even those that have already developed new policies and response plans will have had limited opportunity to test and perfect them. Doing so is vital not only to being prepared but to avoiding the existential threats that cyber threat actors now bring.

CrowdStrike recommends adopting a strong defensive posture by ensuring that remote services, VPNs and multifactor authentication solutions are fully patched and properly integrated, and by providing security awareness training for employees working from home.

PROTECT

Organizations need to have technology solutions that can respond to the rapidly changing landscape. With the cloud-native CrowdStrike Falcon® platform, organizations can take advantage of the scalability and cost-effectiveness of the cloud; protect every endpoint, even those outside of the firewall or offline; use a single lightweight agent to have visibility over every device; and choose to harness CrowdStrike Falcon Complete™ to outsource the implementation, management and incident response of your endpoint security to CrowdStrike's team of security experts.

CrowdStrike recommends adopting a strong defensive posture by ensuring that remote services, VPNs and multifactor authentication solutions are fully patched and properly integrated, and by providing security awareness training for employees working from home.

ABOUT CROWDSTRIKE

CrowdStrike® Inc. (Nasdaq: CRWD), a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches.

The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the organization, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 3 trillion endpoint related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform.

There's only one thing to remember about CrowdStrike: **We stop breaches.**

METHODOLOGY

The CrowdStrike APJ State of Cybersecurity survey was carried out between May 26 and June 7, 2020.

This research surveyed 2,017 business leaders (those in managerial positions; C-suite/executive leadership, senior management and middle management) in Australia, Hong Kong, India, Indonesia, Japan, Malaysia, New Zealand, Philippines, Singapore and Thailand on threats, opportunities, investment and what business recovery post-COVID-19 could look like.

Speak to a representative to learn more about how CrowdStrike can help you protect your environment:

Email: sales@crowdstrike.com
Web: www.crowdstrike.com