Cybersecurity — Keeping Up Pace

The cybersecurity landscape is constantly changing, with vast amounts of data and information being created, new technologies emerging and threat actors developing more sophisticated attack methods. The rise of digitisation and automated workflows also results in the danger of the unauthorised disclosure of information and access to company systems, with the potential of significant legal and financial damage.

Consequently, General Counsel in the Asia region have become increasingly focused on how to advise on the legal implications of cybersecurity attacks.

In fact, almost two-thirds (64%) of respondents agree that their company is not doing enough to proactively reduce cybersecurity risks.

However, when it comes to outside parties, 97% of respondents say they are very confident or quite confident they understand their company's third-party cybersecurity risk and the implications should a connected entity suffer an incident, even when almost half (45%) say their companies do not have a specific third-party risk assessment to capture security and operational risk concerns.

Potential reasons include a lack of available and experienced resources to conduct the assessments, a lack of communication and understanding between different business units and, in some situations, an absence of regulatory requirements for third-party assessments.

In terms of managing cybersecurity risk, 73% of respondents rely on proactive controls, while 69% rely on reactive measures. Proactive controls can include incident response plans, security awareness training of staff, controlling access to systems to only the minimum level necessary, secure infrastructure design and implementation, active security log and event monitoring, threat intelligence monitoring, vendor risk management and regulatory compliance. Reactive controls often cover forensic analysis of what has occurred, back-up and recovery and patch management.

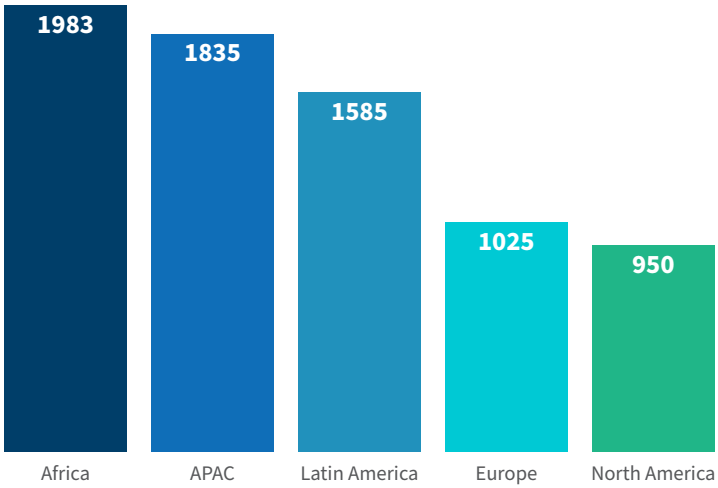
General Counsel are likely to share responsibility for cybersecurity with risk, information technology ("IT"), and compliance departments, meaning it is essential for General Counsel to understand the nuanced cybersecurity risks their organisations are facing and their legal ramifications. This is especially important in the Asia region, where the average number of weekly attempted cyber attacks during the first quarter of 2023 averaged 1,835 per organisation, while the global average stood at 1,248.[1]

The legal ramifications of a cybersecurity incident for companies in the Asia region vary from jurisdiction to jurisdiction, but can include mandatory reporting under personal data legislation, fines for data privacy breaches, civil litigation for financial losses or identity theft, and potential criminal litigation if prosecutors determine that an incident was deliberate.

The organisations with the best cybersecurity posture involve stakeholders throughout, and even outside, the organisation when crafting a cybersecurity and incident response plan. The General Counsel can start with understanding their firm's risk profile and conducting a vulnerability assessment to identify gaps. Testing the crisis response plan on a regular basis is essential; this allows participants to develop an understanding of their roles and identify weaknesses in the plan.

Building a culture of trust and transparency will encourage employees throughout the organisation to communicate concerns without fear of reprisal. The General Counsel can help ensure there are regular check-ins and open lines of communication between stakeholders, breaking down fiefdoms across an organisation where varied approaches to data and cybersecurity can increase risk.

CYBER ATTACKS PER REGION



Data Source: Check Point Research[2]

For more information please contact:

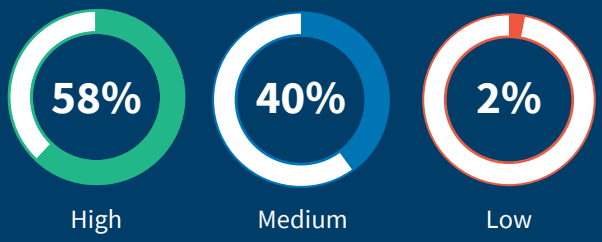
EVA KWOK
Cybersecurity
Senior Managing Director
eva.kwok@fticonsulting.com

[1] Vivek Gullapalli, "Why is the Asia Pacific region a target for cybercrime - and what can be done about it?," World Econonic Forum (12 Jun 2023), https://www.weforum.org/agenda/2023/06/asia-pacific-region-the-new-ground-zero-cybercrime/.

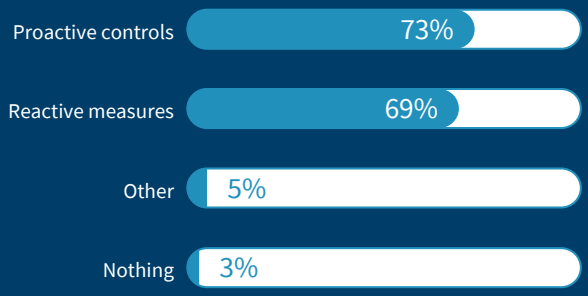
[2] "Global Cyberattacks Continue to Rise with Africa and APAC Suffering Most," Check Point Research (27 April 2023), https://blog.checkpoint.com/research/global-cyberattacks-continue-to-rise/.

Cybersecurity: Survey Findings

What level of priority is cyber preparedness given within your team/company?



What does your company have in place for managing cybersecurity risk?



Which departments are responsible for cybersecurity risk in your company?

71% Legal

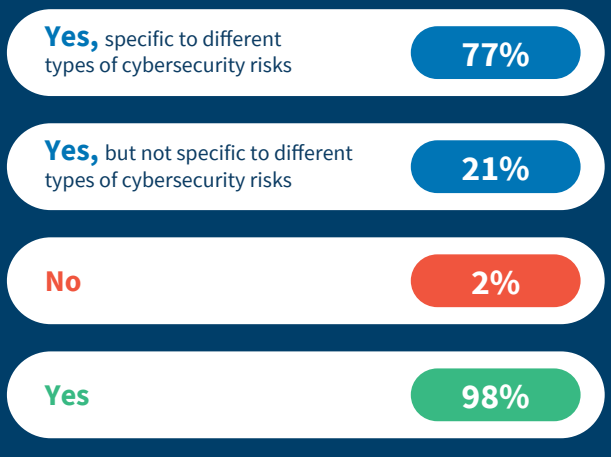
47% Risk

46% IT

36% Compliance

2% Other

Does your company have regularly-tested incident response plans relating to cybersecurity risks?



How confident are you that you understand your company's third-party cybersecurity risk and the implications to your company should a connected entity suffer an incident?