INDEPTHFEATURE

CYBER SECURITY & RISK MANAGEMENT

2022

FINANCIER WORLDWIDE corporatefinanceintelligence

Published by
Financier Worldwide Ltd
First Floor, Building 3
Wall Island, Birmingham Road
Lichfield WS14 0QP
United Kingdom

Telephone: +44 (0)121 600 5910
Email: info@financierworldwide.com

www.financierworldwide.com

Whilst every effort is made to ensure the accuracy of all material published in Financier Worldwide, the publishers accept no responsibility for any errors or omissions, nor for any claims made as a result of such errors or omissions.

Views expressed by contributors are not necessarily those of the publisher.

Any statements expressed by professionals in this publication are understood to be general opinions and should not be relied upon as legal or financial advice.

Opinions expressed herein do not necessarily represent the views of the author's firm or clients or of any organisations of which the author is a member.

FINANCIER
WORLDWIDE corporatefinanceintelligence

INDEPTHFEATURE

CYBER SECURITY & RISK MANAGEMENT

March 2022

Introduction

The frequency and severity of cyber attacks have steadily intensified in recent years. Boosted by increasingly sophisticated tactics and the use of cutting-edge technology, malicious actors have prospered.

In addition to the threats posed by cyber criminals, companies also face regulatory challenges. Maintaining compliance in a landscape where there is no universal standard across jurisdictions for data privacy and protection requires multinational companies to remain nimble. The process can be expensive and time consuming.

In light of the increased threats they face, there are many steps companies can take to protect themselves, their data and their stakeholders. While robust cyber security frameworks are a must, cyber insurance also has a key role to play. Though the cost of cyber insurance is increasing, and it is no substitute for strong network defences, companies that choose to overlook cyber insurance in the current climate may be severely disadvantaged in the event of a successful attack.

Given the number of high-profile cyber breaches reported in recent years and the increased regulatory focus on cyber risk management, the issue is sure to remain a firm fixture on boardroom agendas.

CONTENTS

Financier Worldwide canvasses the opinions of leading professionals on current trends in cyber security & risk management.

UNITED STATES

Guidehouse

Respondents

DONALD HECKMAN
Director
Guidehouse
dheckman@guidehouse.com

Donald Heckman, a cyber security subject matter expert, is a director in Guidehouse's Advanced Solutions. He is the Defense Cyber Solutions Leader developing and leading strong cyber security offerings for defence sector clients. He works with defence clients on all aspects of cyber, ranging from innovative approaches to cyber strategy, policy, security architecture and engineering, to initiatives such as secure IT modernisation, risk management framework (RMF) transformation, identity and access management evolution, weapon system cyber security, secure information sharing and data protection. Additionally, he leads the Cybersecurity Solution's data protection and privacy offerings for public and commercial sector clients.

JACK O'MEARA
Director
Guidehouse
jomeara@guidehouse.com

Jack O'Meara is a director in the Guidehouse Advanced Solutions Cybersecurity practice and leads the Cyber Incident Prevention and Response, and Cyber Litigation Support service offerings. He advises and collaborates with clients to effectively prepare for and respond to cyber incidents, restore operations and develop and deliver cyber resilient solutions, as well as provides litigation support related to cyber intrusions and data breaches. He brings over 30 years of cyber security risk management and operational experience working with various commercial companies and public sector agencies.

Guidehouse

Q. How would you summarise today's cyber risk environment? What new risks have emerged in the past 12-18 months?

A. From a risk impact perspective, the environment remains the same, but the frequency of attacks has increased dramatically. Cyber criminals are still using phishing, ransomware and watering hole attacks to compromise their victims. The lack of patching, insecure IT platform configurations and untrained personnel continue to leave organisations' cyber attack surfaces vulnerable to cyber criminals. Just as cyber defenders are leveraging artificial intelligence (AI) and machine learning (ML) to improve cyber security defences and detect malicious behaviour quickly, cyber criminals are using AI and ML to create more sophisticated cyber attacks while avoiding detection. As a result, ransomware attacks will continue to increase, the IT product supply chain will continue to be targeted and compromised, and a new focus on cryptocurrency exchanges will likely emerge.

Q. What demands are data privacy laws placing on companies in the US to implement security measures and follow notification requirements? How challenging is it to maintain regulatory compliance?

A. Maintaining regulatory compliance can pose significant challenges to companies, given there is no uniform global privacy standard. Companies must stay abreast of, and ensure compliance with, the often-disparate laws and regulations in every country where they operate. The US adds additional complexity with no single national privacy law, but rather a combination of disparate federal and state laws. These tend to focus on type of data, such as health or credit data, or specific population segment, such as students, children, and so on. Without a uniform and prescriptive privacy standard, companies are struggling to ensure compliance, ultimately increasing the cost of privacy programmes. While large companies can more easily absorb increased privacy programme costs, smaller companies may sacrifice investment and innovation funding. In 2019, a report prepared for the California attorney general's office estimated the California Consumer Privacy Act (CCPA) that went into effect on 1 January 2020, one of the more comprehensive privacy laws in the US, would cost $55bn in aggregate for California companies to comply.

Q. Would it be fair to say that, in general, organisations are still not up to speed on detecting security breaches and privacy risks quickly enough?

A. According to IBM Security's 'Cost of a Data Breach Report 2021', the average time to identify a breach in 2021 was 212 days and the average time to contain a breach was 80 days. This would indicate that many organisations are still not performing even basic IT cyber security hygiene, such as asset management, configuration management, patching, vulnerability management and security awareness and training. The lack of these processes and policies are a root cause of many major cyber attacks over the past two decades.

Q. What steps should companies take to establish appropriate processes and policies to manage cyber-related risks and keep systems safe?

A. Implementing a holistic cyber security programme using defence-in-depth, combined with a zero-trust framework, is the best way to keep systems and data safe. A thorough set of IT cyber security hygiene processes is critical to any cyber security programme. Every user should be required to use multifactor authentication. Privilege access management should be implemented to provide only those job or account privileges that are essential to performing its intended function. All the assets should be securely configured and monitored to ensure they are running the most current and patched software. Finally, as most breaches are a result of human error, companies need to build an enterprise-wide cyber risk-aware culture.

Q. How are insurance providers enhancing their cyber insurance solutions to meet market demands and help companies manage the downside?

A. Given the exponential growth in ransomware attacks, cyber insurance is becoming more expensive, demanding that companies implement and maintain more robust cyber security programmes. The burden of proof to demonstrate sustained

Guidehouse

compliance with required security controls has shifted from the insurance companies to the insured. Finally, several cyber insurance companies have signalled they will no longer pay ransoms but will only cover the direct cost of business impact and recovery.

Q. What considerations should companies make when evaluating cyber insurance coverage, including pricing, policy provisions and exclusions?

A. Before evaluating insurance coverage, companies need to understand their cyber risks. Companies are using outdated, unreliable approaches to cyber risk management. These approaches are proving insufficient, resulting in recent high-profile breaches. Companies must start quantifying cyber risk to truly understand the potential business risk and associated financial losses. Using cyber risk quantification techniques enables companies to identify cyber risks, estimate their financial impact, and evaluate how this impact might be offset by financial controls, including risk transfer to the appropriate cyber insurance, including pricing, provisions and exclusions.

> *Companies must stay abreast of, and ensure compliance with, the often-disparate laws and regulations in every country where they operate.*

Guidehouse

Q. Going forward, do you expect cyber risk management will continue to climb the boardroom agenda as a major issue?

A. Cyber risk management will continue to climb the boardroom agenda if cyber attacks continue to be successful and pervasive. Given the high-profile ransomware attacks across the globe, many countries, including the US, have enacted, or are in the process of creating, new cyber security requirements and privacy regulations, such as the US Executive Order on Improving the Nation's Cybersecurity in May 2021. These new regulations put the onus of ensuring compliance and accountability for cyber risk on the C-suite. This makes it critical for cyber security executives to communicate cyber risk in terms of potential business impact to garner the attention of company executives – this information must enable the C-suite to make actionable and informed decisions. To do so, cyber security executives must be able to quantify the potential impact of cyber risk. By quantifying the organisation's cyber risk, security leaders will have the information they need to demonstrate potential incident impact to leadership, including financial and reputation damage and legal repercussions. ❑

Guidehouse

www.guidehouse.com

GUIDEHOUSE is a leading global provider of consulting services to the public and commercial markets with broad capabilities in management, technology and risk consulting. The firm helps clients address their toughest challenges with a focus on markets and clients facing transformational change, technology-driven innovation and significant regulatory pressure. Across a range of advisory, consulting, outsourcing, and technology and analytics services, Guidehouse helps clients create scaleable, innovative solutions that prepare them for future growth and success.

DONALD HECKMAN Director
dheckman@guidehouse.com

JACK O'MEARA Director
jomeara@guidehouse.com

Guidehouse

CANADA

Norton Rose Fulbright Canada LLP

Respondents

IMRAN AHMAD
Partner
Norton Rose Fulbright Canada LLP
+1 (416) 202 6708
imran.ahmad@nortonrosefulbright.com

Imran Ahmad is the Canadian head of Norton Rose Fulbright's technology and innovation industry group and the Canadian co-head of the firm's data protection, privacy and cyber security practice. He is recognised as a leading cyber security lawyer by several legal directories. He advises clients on a wide array of technology-related matters, including outsourcing, cloud computing, SaaS, strategic alliances, technology development, system procurement and implementation, technology licensing and transfer, distribution, open source software, and electronic commerce. As part of his cyber security practice, he works closely with clients to develop and implement practical strategies related to cyber threats and data breaches.

TIANA COROVIC
Associate
Norton Rose Fulbright Canada LLP
+1 (416) 216 2448
tiana.corovic@nortonrosefulbright.com

Tiana Corovic is an associate in the firm's Toronto office with a focus on privacy, regulatory compliance, technology, data protection, and mergers and acquisitions. As part of her practice, she also advises clients on cyber breach management and third-party data processing agreements.

Norton Rose Fulbright Canada LLP

Q. How would you summarise today's cyber risk environment? What new risks have emerged in the past 12-18 months?

A. Over the last two years, we have seen a significant change in the cyber landscape, both in Canada and globally. Following the sudden shift to working remotely in March 2020, many organisations had to implement new solutions and technology as quickly as possible. The increase in the number of cyber incidents seen in 2020 was not a temporary effect while organisations adjusted to a new work environment; instead, it has become a trend that has stabilised across Canada. In early 2022, we saw an increase in business email compromises where entire mailboxes have been synced to an external device. Additionally, ransomware attacks, which are merely a subset of cyber incidents, have greatly evolved over the past few months. Threat actors have begun to realise the value of data by going after crown jewels rather than stealing data indiscriminately. Malicious actors have gone after cyber insurance policies among other sensitive data that gives them an upper hand during ransom negotiations.

Q. What demands are data privacy laws placing on companies in Canada to implement security measures and follow notification requirements? How challenging is it to maintain regulatory compliance?

A. In Canada, notification requirements depend on the type of organisation that is impacted. In the private sector, we see a 'real risk of significant harm' threshold that triggers notification requirements to both regulators and impacted individuals. The timing for notifications, be it 'without unreasonable delay' or 'as soon as feasible', often ends up being a judgment call depending on the type of data that has been compromised and the likelihood of misuse, information that may not be available until a forensic investigation is well underway. In other cases, we may see more strictly defined timelines, for example, federally regulated financial institutions must submit an initial report to the Office of the Superintendent of Financial Institutions 24 hours or sooner after a security incident. Finally, we may see some indirect notification requirements that arise from provincial securities laws where a public offering company must

Norton Rose Fulbright Canada LLP

> A thorough set of IT cyber security hygiene processes is critical to any cyber security programme. Every user should be required to use multifactor authentication.

publish a news release 10 days following a cyber incident that is deemed a 'material change'.

Q. Would it be fair to say that, in general, organisations are still not up to speed on detecting security breaches and privacy risks quickly enough?

A. As technology advances, so too does the sophistication of cyber attacks. The average dwell time between the initial intrusion and deployment of ransomware is about three days. This is enough time for the threat actor to steal credentials, exfiltrate significant amounts of data and set up backdoors to exploit at a later date. In most cases, ransomware is executed over the weekend or after hours, such that the initial compromise may be completed under 24 hours without raising an alarm. On the other hand, business email compromises may also be challenging to detect because threat actors will often set up mailbox rules that might, for example, move emails from a specific sender to the read or deleted folder. It could take weeks before the user realises their account has been compromised.

Norton Rose Fulbright Canada LLP

Q. What steps should companies take to establish appropriate processes and policies to manage cyber-related risks and keep systems safe?

A. Preparation impacts response. Organisations are encouraged to develop a cyber incident response plan (CIRP) to quickly respond to and manage cyber-related risks. Some aspects to consider in your CIRP include contact information for your cyber insurer, breach counsel and response team, triggers that help identify a threat as it is not always as obvious as a ransom note displayed on a desktop, and delegating responsibilities between members of your organisation, including who can make the call to take systems offline before an encryption event spreads. Given the increase in ransomware payments, we have also begun to see a greater demand for ransomware playbooks as standalone documents that set out a decision tree on how and when to negotiate. Your response plans should be available as physical copies in the event a cyber incident limits accessibility to online documents. When it comes to everyday risk management policies, companies should set out data retention requirements to minimise their digital footprint and regular cyber training sessions, at a minimum. To the extent you are relying on third-party vendors, consider putting in place contractual provisions that list minimum safeguard requirements and breach notification requirements.

Q. How are insurance providers enhancing their cyber insurance solutions to meet market demands and help companies manage the downside?

A. Cyber insurance went from being an add-on to errors & omissions policies to a standalone document covering third-party costs in the late 1990s. When Canada's first breach reporting requirements came out in Alberta in 2010, insurers responded by expanding coverage to include, for example, the cost of response teams and notifications. With ransomware attacks reaching a new high, we may begin to see insurers moving away from paying a ransom due to the growing concern that it could lead to more demands in the future. The cost of insurance has also evolved over the years by placing a greater emphasis on the type of data organisations collect that could present a real risk as opposed to focusing on projected revenue. As insurance renewals come up, organisations are being asked difficult questions regarding their security posture to properly assess the cost and scope of coverage.

Q. What considerations should companies make when evaluating cyber insurance coverage, including pricing, policy provisions and exclusions?

A. Cyber insurance typically covers business interruption costs, for example when an encryption event halts the delivery of services and backups are either outdated or take time to restore. Depending on the policy, the level of coverage may extend to restoring an organisation's system to its pre-breach state. Additionally, cyber insurance can cover the costs of your response team, ransom payments, defence against lawsuits, recovering data, notifications and regulatory investigations, to name a few. If you are storing data on third-party platforms, such as the cloud, you may want to consider whether your insurance will cover third-party breaches. Common exclusions from cyber insurance include audits of an organisation's security posture, costs associated with implementing additional safeguards, and security incidents facilitated by an insider. Moreover, physical breaches, such as fried computers, exploited phone systems or security cameras that need to be replaced, are also typically not covered by cyber insurance. It is important to consider the type of cyber insurance that will best suit your IT infrastructure and its ensuing risks to mitigate some of the astronomical costs that can follow a security incident.

Q. Going forward, do you expect cyber risk management will continue to climb the boardroom agenda as a major issue?

A. We anticipate cyber risk management will become a more common topic in boardroom discussions for various reasons. For one, we see ramifications following a cyber incident that include possible litigation, financial loss from having to pay a ransom and having to restore the IT environment, and a turnover of senior management. More specifically, for public offering companies, a cyber incident could lead to a significant effect on the market price or value of their securities that will need to be reported in

Norton Rose Fulbright Canada LLP

a news release. Cyber incidents are gaining increasing traction in media coverage that is bringing a new level of awareness that no one can be 100 percent immune from a cyber attack. Organisations can engage in vicarious learning by avoiding the same financial and reputational repercussions that have befallen others. ❑

www.nortonrosefulbright.com

NORTON ROSE FULBRIGHT is a global law firm which provides the world's preeminent corporations and financial institutions with a full business law service. The firm has more than 3700 lawyers and other legal staff based in more than 50 cities across Europe, the United States, Canada, Latin America, Asia, Australia, the Middle East and Africa. Recognised for its industry focus, the firm is strong across all the key industry sectors: financial institutions; energy; infrastructure and resources; transport; technology; life sciences and healthcare; and consumer markets.

IMRAN AHMAD Partner
+1 (416) 202 6708
imran.ahmad@nortonrosefulbright.com

TIANA COROVIC Associate
+1 (416) 216 2448
tiana.corovic@nortonrosefulbright.com

NORTON ROSE FULBRIGHT

UNITED KINGDOM

S-RM

Respondents

LENOY BARKAI
Director
S-RM
+44 (0)20 3763 9595
hello@s-rminform.com

Lenoy Barkai co-leads S-RM's Cyber Advisory practice. She has over nine years' experience spanning security risk analysis, strategic consulting and alternative investment management. Since joining S-RM in 2018, she has supported clients working through complex cyber and physical security challenges, and has led projects spanning the private equity, extractives and FMCG industries, among others. Prior to joining S-RM, she worked as a consultant to the global philanthropy team at the International Secretariat of Amnesty International in London and was regional head of research at a global wealth advisory firm, where she managed a portfolio of alternative investment funds.

MIKE GROVES
Director
S-RM
+44 (0)20 3763 9595
hello@s-rminform.com

Mike Groves co-leads S-RM's Cyber Advisory practice, working with clients from a diverse range of sectors, to make their organisations more resilient to cyber security risks. He joined S-RM's Crisis Management Team in 2015 as a corporate security operations manager focusing on the provision of terrorism and political violence response services. He subsequently led the development of S-RM's crisis preparedness functions for corporate clients from a range of sectors and developed specialisms in the design and delivery of emergency management exercises. Before joining S-RM, he spent five years in the British Army, leaving at the rank of captain.

S-RM

Q. How would you summarise today's cyber risk environment? What new risks have emerged in the past 12-18 months?

A. Although the objectives of cyber criminals have remained constant – maximising profits while minimising efforts – cyber attacks over the previous 12-18 months have exemplified the increasing levels of sophistication among criminal gangs. Ransomware operators, who continue to pose the most prominent risks to organisations, have added new weapons to their arsenals to enhance the likelihood of receiving a payout. Tactics include leveraging double encryption attacks, in which victims' data is encrypted with two or more, rather than a single, ransomware strains. Distributed denial of service (DDoS) attacks have taken victims' websites offline until a ransom has been paid, causing major business interruption. And increasingly we have seen instances of attackers cold-calling victims to apply pressure if ransom demands have been ignored.

Q. Would it be fair to say that, in general, organisations are still not up to speed on detecting security breaches and privacy risks quickly enough?

A. In our recent survey of 600 C-Suite and IT budget holders from across the US and UK, only 40 percent of respondents thought their organisation would be 'completely successful' at detecting a cyber incident. The same respondents thought their organisations could be more successful with better employee appreciation of cyber security risks, and greater understanding of breach response policies. These two points were backed up by a third area, also centred around people: cultivating a security-positive culture. When every single one of an organisation's employees is educated and empowered to detect and respond to cyber security vulnerabilities, that organisation can move to hardening its technical infrastructure.

Q. What steps should companies take to establish appropriate processes and policies to manage cyber-related risks and keep systems safe?

A. Companies should begin by defining the objectives of their information security function – looking at which information assets and systems they are trying to protect the confidentiality, integrity and availability of, and why. Next, build out the cyber security policy, which should describe the 'ideal state' of the domain outlined in the objectives. Then supplementary procedures can be written, detailing how the ideal state is to be reached and maintained. If you are aiming to align with, or attain compliance with, a particular industry standard or framework, ensure that your policies define an ideal state that meets these requirements. Finally, engage employees with the policies and procedures so they understand their role and the consequences of not adhering to policy, even in the case of accidental policy violations.

Q. What are the typical legal impacts of an incident and some of the costs associated with those impacts?

A. For organisations that have not implemented 'reasonable' data protection measures in the eyes of regulators, the legal implications of a breach may be more harmful than the financial and reputational impacts. The EU's General Data Protection Regulation (GDPR) is commonly thought of when considering this, but the rest of the world is catching up and non-European countries are using GDPR as a model to protect their own citizens. Organisations must ensure that they put effort into protecting their consumers' data to avoid penalties. Even reporting an incident to a regulator may prove to be expensive. Often, the burden of proof rests on the shoulders of the impacted organisation. Third-party response and forensic providers must be brought in to assess the extent of the damage for regulators to make accurate judgements, which can be an expensive process, particularly if attackers have erased evidence of their activities. Finally, customers impacted by the incident may assert a claim against the organisation. With enough claimants, this can lead to a class action lawsuit resulting in significant financial and reputational damage.

Q. What are your observations on the hardening of the cyber insurance market and the steps that companies are taking to achieve insurance?

S-RM

A. Harder market conditions have set in over the past six to 12 months across the cyber insurance market. These conditions have driven increases in premiums and resulted in a reduction in capacity, as many carriers look to rebalance portfolios toward excess layers rather than take on too much primary exposure. In practical terms, the harder market means that underwriters are using more exhaustive and detailed applications to assess applicants' cyber security postures. Gone are the days when prospective insureds could expect to receive insurance without attesting to, and evidencing, robust controls on cyber security basics like multifactor authentication (MFA), backups provision, adequate remote access configuration, privileged network access and robust network segmentation, to name a few.

Q. What steps are companies taking to improve their preparedness for cyber attacks?

A. There are many options available to companies ready to invest in their cyber security preparedness. In a market where being able to transfer the risk to insurance

> *Update and simplify the incident response plan and make sure it works by exercising staff and processes with a simulated attack – these do not have to be long or expensive to arrange.*

S-RM

is no longer a foregone conclusion, and simply ignoring it is a disaster waiting to happen, companies are increasingly focusing on their responsibility to build meaningful resilience from within. In practice, that means taking a number of steps. First, companies need to map their IT environments and attack surfaces. You cannot protect what you cannot see or do not know is vulnerable. Second, take the time to fully understand the efficacy of the existing controls in place – carry out a comprehensive assessment to map the existing mitigation, and identify the gaps in technical and governance controls. These steps will build the foundations for an effective 'road mapping' exercise in which solutions can be intelligently focused on known and prioritised weaknesses. Implementation must be owned at the right level of leadership and resourced with appropriate expertise. If there is not time or budget to go through these steps, assume that an attack is likely to happen sooner rather than later and focus on quick wins. Ramp up the response arrangements in place. Update and simplify the incident response plan and make sure it works by exercising staff and processes with a simulated attack – these do not have to be long or expensive to arrange. Organise penetration testing to expose and remediate the flaws most visible to would-be attackers. Finally, address your biggest vulnerability by providing security awareness training for your staff.

Q. Going forward, do you expect cyber risk management will continue to climb the boardroom agenda as a major issue?

A. Cyber risk has become an increasingly prominent line item on the boardroom agenda. Board members of leading organisations have recognised that cyber risk is not the sole purview of IT teams, or even of chief information security officers. It is a business-critical risk that needs to be managed with the same level of attention and sensitivity that 'traditional' risk factors have been given for years. Our 2021 survey of 600 C-suite and senior IT leaders revealed that 54 percent considered their board members to be "totally proactive" when it came to cyber security. In other words, cyber risk was considered a high priority and was a frequent topic of conversation in the boardroom. A further 38 percent described their boards as "slightly proactive", indicating that cyber was registering on the agenda, but not to a full enough extent. Only 7 percent of respondents described their boards as reactive: either not taking the initiative to pre-emptively manage cyber risk or only dealing with it in the event of an incident. The most mature leadership teams take their approach to cyber security a step further: from risk management to competitive advantage. ❑

www.s-rminform.com

S-RM is a global intelligence and cyber security consultancy. Founded in 2005, the firm has more than 250 experts and advisers across six international offices. The firm provides intelligence that informs critical decisionmaking and strategies, from investments and partnerships through to disputes. The firm helps its clients exploit opportunities and navigate complex risks globally.

LENOY BARKAI Director
+44 (0)20 3763 9595
hello@s-rminform.com

MIKE GROVES Director
+44 (0)20 3763 9595
hello@s-rminform.com

RODDY PRIESTLEY Director
+44 (0)20 3326 8108
r.priestley@s-rminform.com

S-RM

FRANCE

Gibson, Dunn & Crutcher LLP

Respondent

AHMED BALADI
Partner
Gibson, Dunn & Crutcher LLP
+33 (0) 1 56 43 13 00
abaladi@gibsondunn.com

Ahmed Baladi is a partner in the Paris office of Gibson, Dunn & Crutcher LLP and the co-chair of the firm's Privacy, Cybersecurity and Data Innovation Practice Group. He specialises in information technology and digital transactions, outsourcing, data privacy and cyber security. He has developed considerable experience in a wide range of technology and digital matters. His practice covers complex technology transactions and outsourcing projects, particularly in the financial institutions sector.

Gibson, Dunn & Crutcher LLP

Q. How would you summarise today's cyber risk environment? What new risks have emerged in the past 12-18 months?

A. The most important cyber risk that companies face today is ransomware attack. This risk is even more acute with the increasing use of mobile and personal devices by employees, and the availability of tools, kits and structures to carry out ransomware attacks. This trend has been reinforced by remote working practices which many organisations have had to rely on during the coronavirus (COVID-19) pandemic. As remote working has become more widespread, companies have been exposed to increased numbers of security threats deriving from remote worker endpoints and cloud jacking. Phishing attacks also constitute a common risk since organisations continue to lack awareness and readiness to mitigate the effects of such attacks. Therefore, we cannot say that there are necessarily new risks, but there has been an increase in the frequency and efficiency of existing cyber attacks that impact all organisations across all sectors.

Q. What demands are data privacy laws placing on companies in France to implement security measures and follow notification requirements? How challenging is it to maintain regulatory compliance?

A. First, the EU's General Data Protection Regulation (GDPR) requires companies to focus on establishing technical and organisational measures to prevent or mitigate security threats. Companies should also implement measures that enable early detection of data security breaches. Companies should also ensure they have adequate incident response plans which allow them to notify relevant authorities of security incidents in a timely manner. The biggest challenge for companies is maintaining regulatory compliance with all applicable legislation. Companies tend to focus on the GDPR but other legislation could apply, such as the EU Security of Networks & Information Systems (NIS) Directive, which also imposes obligations to notify national security or cyber security authorities, as well as other regulations in jurisdictions where companies operate. Furthermore, specific sector-focused regulations or guidelines may apply. Navigating through these legal environments and having to

Gibson, Dunn & Crutcher LLP

> *Companies are increasingly utilising cyber insurance. However, the market is still relatively immature, there is a lack of consistency in insurance offerings and prices are very high.*

deal with various authorities for the same incident is extremely challenging.

Q. Would it be fair to say that, in general, organisations are still not up to speed on detecting security breaches and privacy risks quickly enough?

A. Companies are still learning how to navigate different legal requirements, whether they arise from the GDPR, the NIS Directive or any other sector-specific legislation. It is fair to say that many organisations are still not up to speed on detecting security breaches quickly enough. Companies also struggle to understand whether or not a security incident needs to be reported. Relying on more resources, either internally or externally, would certainly help.

Q. What steps should companies take to establish appropriate processes and policies to manage cyber-related risks and keep systems safe?

A. Companies should rely on available expertise. Before launching a project, companies should understand their environment, including any suppliers

Gibson, Dunn & Crutcher LLP

and third parties they rely on to conduct their operations. Considering this security mapping, companies should be able to identify and implement preventive measures to protect against potential data security breaches and other cyber-related risks. In addition to the procedures and policies required by applicable regulations, it is also necessary to implement technical measures. This may include encrypting data at rest and in transit, engaging a third-party to audit information systems and networks, and using tools to enable early detection of security incidents.

Q. How are insurance providers enhancing their cyber insurance solutions to meet market demands and help companies manage the downside?

A. Because remedial actions resulting from data privacy and security violations can be costly, companies are increasingly utilising cyber insurance. However, the market is still relatively immature, there is a lack of consistency in insurance offerings and prices are very high. In addition, some companies may wrongly believe that their insurance policy will protect them against all risks arising from a cyber incident, whereas exclusions apply. Whether it is advisable for a company to adopt insurance services depends on the specific sector and the data processing activities at issue.

Q. What considerations should companies make when evaluating cyber insurance coverage, including pricing, policy provisions and exclusions?

A. Companies need to be conscious of key factors, such as the categories of personal data they are processing or subject to their control, the types of processing operations undertaken, the risks and security measures implemented, and their level of compliance with data protection and data security regulations. For example, a company may conclude that it processes highly sensitive personal data, or that, despite its security measures, it is highly exposed to data breaches that could have a significant impact on users. In these cases, companies may seek cyber insurance to protect themselves from losses related to customer service claims, damages claims or sanctions. Prior to obtaining cyber insurance, companies should enhance their compliance measures and compare

Gibson, Dunn & Crutcher LLP

insurance coverage and pricing to reduce their premiums.

Q. Going forward, do you expect cyber risk management will continue to climb the boardroom agenda as a major issue?

A. Cyber and data security are likely to remain a top priority. Political instability around the globe may increase the number of state-sponsored attacks. In addition, the prevalence of remote and mobile working extends security exposures to remote worker endpoints. Finally, lucrative ransomware attacks will continue to encourage attackers. In addition to cyber attacks, companies also face the risk of being sanctioned by the relevant authorities for failing to implement appropriate security measures. For these reasons, cyber risk management will continue to climb boardroom agendas as a critical issue. ❑

www.gibsondunn.com

GIBSON, DUNN & CRUTCHER has more than 1600 lawyers in 20 offices in major cities throughout the US, Europe, the Middle East, Asia and South America. The firm is committed to providing the highest quality legal services to its clients. In Europe, the firm's established, internationally networked group of qualified US, English, French, Spanish and German lawyers has considerable experience in representing clients with international business interests that require a coordinated and seamless response within and across European national borders.

AHMED BALADI Partner
+33 (0) 1 56 43 13 00
abaladi@gibsondunn.com

GIBSON DUNN

BELGIUM

Gibson, Dunn & Crutcher LLP

Respondent

ALEJANDRO GUERRERO
Of Counsel
Gibson, Dunn & Crutcher LLP
+32 2 554 72 18
aguerrero@gibsondunn.com

Alejandro Guerrero is of counsel in the Brussels office of Gibson, Dunn & Crutcher, specialising in EU competition, data protection and technology law and regulation. He has broad experience in general EU antitrust and its interaction with intellectual property, cartel enforcement, vertical agreements, abuse of dominance and antitrust private litigation. He has advised a variety of clients active in the luxury, financial, technology, energy, consumer goods and telecommunications sectors, including working as secondee for some clients.

Gibson, Dunn & Crutcher LLP

Q. How would you summarise today's cyber risk environment? What new risks have emerged in the past 12-18 months?

A. Companies continue to be exposed to traditional cyber threat attacks, such as phishing, ransomware, malware and insider threats. Approximately one third of successful cyber attacks involve phishing, and phishing is instrumental in two thirds of all cyber attacks. Phishing attacks are likely to continue as people increase their online presence, and the social engineering employed to steal user credentials becomes more elaborate. Cyber attackers are also developing sophisticated phishing attempts launched through cloud applications, which have higher trust levels from users and are therefore more effective. Ransomware and malware also represent a serious threat to cyber victims, given the increasing use of unprotected mobile and home devices by employees, and the availability of tools, kits and structures to enforce ransomware and malware attacks. As remote and mobile working have become a widespread reality since 2020 and 2021, companies are more exposed to security threats deriving from remote worker endpoints and cloud jacking.

Q. What demands are data privacy laws placing on companies in Belgium to implement security measures and follow notification requirements? How challenging is it to maintain regulatory compliance?

A. The EU's General Data Protection Regulation (GDPR) requires companies to focus on the establishment of technical and organisational measures that prevent or hinder the materialisation of security threats. Companies should also implement measures that enable the early detection of data security breaches. For example, monitoring of traffic load, data extraction devices or code detection in outgoing emails can help identify the use of physical and digital means to unduly access and extract data. Finally, companies should put in place adequate response plans and policies, including the involvement of internal or external lawyers with access to the necessary notification requirements. It might sound challenging to maintain these policies and mechanisms, but companies generally achieve this by putting in place accountability and reporting mechanisms, conducting regular training, and performing security and intrusion penetration tests and compliance audits.

Q. Would it be fair to say that, in general, organisations are still not up to speed on detecting security breaches and privacy risks quickly enough?

A. Companies have understood that the GDPR and other sector-specific legislation, such as the Security of Networks and Information Systems (NIS) Directive, require them to enhance their duties of confidentiality and cyber security. Companies also understand that they need to minimise risks that could lead to reportable data breaches. However, some companies may still need to fully comprehend and assimilate the breadth of the definition of potential security breaches and privacy risks deriving from certain processing practices. For example, the internal availability of plain text security information, the absence of internal access rules and barriers to access databases, and other similar gaps in GDPR compliance may lead to violations, either in and of themselves or due to the facilitation of more serious security breaches, such as

> *"As remote and mobile working have become a widespread reality since 2020 and 2021, companies are more exposed to security threats deriving from remote worker endpoints and cloud jacking."*

Gibson, Dunn & Crutcher LLP

data theft or loss. Some organisations still need to get up to speed in this regard.

Q. What steps should companies take to establish appropriate processes and policies to manage cyber-related risks and keep systems safe?

A. Companies should first adopt preventive measures to protect against potential data security breaches and other cyber-related risks. These measures can comprise both technical and organisational measures that deter or hinder the materialisation of security threats, such as two-factor authentication to access sensitive or vulnerable systems. The storage of personal data and information in remote, standalone, archives or backup systems is a good means of ensuring the preservation and availability of recoverable data in case of loss or theft. Companies should also implement measures that enable the early detection of data security breaches.

Q. How are insurance providers enhancing their cyber insurance solutions to meet market demands and help companies manage the downside?

A. Because remedial action can be costly in the context of data privacy and security violations, in some countries, both outside and within the EU, companies are increasingly turning to cyber insurance services for security and data privacy breach coverage. However, we are still at the dawn of GDPR enforcement, and there is a general absence of consistent and accurate historical data and statistics on security breaches and the value of exposures and damages by sector. In the absence of this type of information, risk transfer and insurance services can prove expensive in the long term. While risk transfer and insurance may increasingly relieve some companies from large exposures, they will not completely remove pre-emptive and reactive costs related to data breaches. Whether it may be advisable for a company to adopt these insurance services depends on the specific activity or sector and the data processing operations at issue.

Q. What considerations should companies make when evaluating cyber insurance coverage, including pricing, policy provisions and exclusions?

Gibson, Dunn & Crutcher LLP

A. Companies should first be conscious of key factors, such as the categories of personal data that they are processing or that is subject to their control, including by third party vendors or processors, the types of processing operations undertaken, the risks and the security measures implemented. These factors should broadly inform a decision whether to proceed and obtain cyber insurance. For example, a company may reach the conclusion that it processes highly sensitive personal data, or that, despite the security measures implemented, it is highly exposed to data breaches that can have a significant impact on users. In these cases, companies may seek cyber insurance to protect themselves from losses related to customer service claims, damages claims or sanctions. Prior to obtaining cyber insurance, companies should enhance their compliance measures and should compare among insurance service prices to reduce their premiums.

Q. Going forward, do you expect cyber risk management will continue to climb the boardroom agenda as a major issue?

A. Cyber and data security are likely to remain at the top of companies' priorities, as remote working trends have become a reality. The prevalence of remote and mobile working is extending security exposures to remote worker endpoints. According to some studies, approximately one quarter of data breaches involve off-premises assets, mobile devices and telecommuters, and this figure is only likely to rise post-pandemic. The increased use of cloud services to cover operations and management also creates a single exposure point for companies. As opposed to identifiable attacks, like ransomware, malware or phishing attacks, cloud jacking attacks are more likely to remain undetected and have long-term negative effects, being used for corporate espionage and copying of data stored in the cloud. The emergence of deep fake software to manipulate existing videos and audio recordings of people also poses a significant threat, especially if combined with traditional phishing attacks. ❑

Gibson, Dunn & Crutcher LLP

www.gibsondunn.com

GIBSON, DUNN & CRUTCHER has more than 1600 lawyers in 20 offices in major cities throughout the US, Europe, the Middle East, Asia and South America. The firm is committed to providing the highest quality legal services to its clients. In Europe, the firm's established, internationally networked group of qualified US, English, French, Spanish and German lawyers has considerable experience in representing clients with international business interests that require a coordinated and seamless response within and across European national borders.

ALEJANDRO GUERRERO Of Counsel
+32 2 554 72 18
aguerrero@gibsondunn.com

GIBSON DUNN

SPAIN

Aon Risk Solutions

Respondent

CLAUDIA GÓMEZ
Executive Director
Aon Risk Solutions
+34 618 686 525
claudiabeatriz.gomez@aon.es

Claudia Gómez is the head of cyber insurance for Spain and Portugal, as well as of the financial & professional solutions specialty in Spain. She has more than 25 years of experience in the insurance industry, helping medium and large organisations to secure complex insurance programmes. In the last 20 years, she has been involved in assessing and placing D&O, crime and professional liability programmes for both commercial and financial institutions, and since 2012 she has been heavily involved in promoting and placing cyber insurance as well as developing and promoting Aon's cyber risk consulting and security capabilities.

Aon Risk Solutions

Q. How would you summarise today's cyber risk environment? What new risks have emerged in the past 12-18 months?

A. The current cyber risk environment is tremendously challenging. Digitalisation and digital transformation has accelerated during the coronavirus (COVID-19) pandemic, so companies are now even more dependent on software and data than before. The pandemic has allowed cyber criminals to increase their attacks against corporations worldwide. In Spain, cyber attacks increased 125 percent in 2021 compared to 2020. Criminals have taken advantage of new critical vulnerabilities, such as 'Log4J', to increase the number and impact of attacks. But the greatest risk has been, and continues to be, ransomware. In the first half of 2021, the number of ransomware attacks surpassed the number recorded in all of 2020. In addition to the alarming frequency and severity of these attacks, it is concerning to see how criminals have changed their tactics. Ransomware is used only to extort, however many cyber criminals are breaching and erasing all types of data, including personally identifiable information (PII) and other confidential data. They are consciously targeting critical and industrial infrastructure to cause severe interruptions. And finally, they are using organisations' IT supply chains to multiply the success of their attacks.

Q. What demands are data privacy laws placing on companies in Spain to implement security measures and follow notification requirements? How challenging is it to maintain regulatory compliance?

A. The General Data Protection Regulation (GDPR) poses challenges to all companies due to the high standards of its requirements, and recently new requirements were imposed for data transfers outside the EU. The challenge is therefore higher for small and medium-sized enterprises (SMEs), which are trying to survive and be profitable in an extremely difficult and competitive economic environment. Many of these companies run the risk and choose not to comply with the GDPR. But we are also seeing larger companies, which are compliant with GDPR, being pressed by regulators to go beyond the basic requirements. Throughout Europe, regulatory sanctioning procedures have increased, both in number and in the size of fines. Spain is among the countries with the highest number of GDPR sanctions, with a 1000 percent increase in the fines levied against companies in 2021 compared to 2020. Most of these fines are related to violations of the general principles of the GDPR, but the fines also relate to security breaches. We expect regulatory scrutiny and requirements to increase in the coming years.

Q. Would it be fair to say that, in general, organisations are still not up to speed on detecting security breaches and privacy risks quickly enough?

A. The current cyber risk environment has elevated cyber attacks and data breaches to the top of most companies' thinking, according to different industry surveys, however the statistics demonstrate that companies are not well prepared to detect and face security threats. Only 40 percent of companies believe they have deployed adequate security controls for remote work during the pandemic, 31 percent report having adequate business resilience measures in place to deal with ransomware, and a 21 percent have baseline measures to oversee critical suppliers and vendors. Many companies still have a long way to go to improve their cyber security management.

Q. What steps should companies take to establish appropriate processes and policies to manage cyber-related risks and keep systems safe?

A. The key step companies should take is to establish a cyber risk management framework on an enterprise-wide basis. Essentially, it should be aligned with all relevant stakeholders within the business to achieve resilience. Industry best practices, as well as regulations, recommend that such a framework should consist of five fundamental pillars. First, assess the cyber threat profile of the company, know the key technology and assets to protect, and review and test existing defences. Second, protect by deploying security technology and processes, and arranging training and incident response readiness to improve the company's defences. Third, detect by developing controls and measures to proactively identify and discover cyber

Aon Risk Solutions

Companies that delay in addressing cyber security should be aware that the evolving environment, both in terms of security threats and regulation, will lead to more claims against companies and their boards.

security events prior to response. Fourth, be ready to effectively respond to a critical incident by having appropriate threat intelligence and other tools, as well as planning and rehearsing incident response plans. Finally, be ready to recover by establishing business continuity and disaster recovery plans for returning to normal business operations as soon as possible while minimising the impact of critical incidents.

Q. How are insurance providers enhancing their cyber insurance solutions to meet market demands and help companies manage the downside?

A. Unfortunately, there have been no enhancements to insurance coverage. The huge increase in the frequency and severity of incidents, of which 58 percent are ransomware-related losses, also hit the insurance market, raising its loss ratios well above 100 percent over the last two years. This situation has led to a very hard cyber insurance market environment. Insurers have adjusted their underwriting approach and continue to do so, requiring more underwriting information, reviewing terms and conditions of coverage, and re-evaluating capacity deployment. This means that restrictions or exclusionary language for ransomware-related attacks or supply chain business interruption cover must mention two of the most relevant changes – minimum premium increases in the region of 35-50 percent, and a relevant reduction of the capacity placed in a single risk to an average of €5m, compared to €15-25m previously.

Q. What considerations should companies make when evaluating cyber insurance coverage, including pricing, policy provisions and exclusions?

A. Any company that wants to secure cyber insurance, either as a new buyer or when renewing an existing cyber insurance programme, should demonstrate to insurers that it has an appropriate level of cyber security maturity. Maturity involves the implementation of proactive risk mitigation strategies, such as business continuity and disaster recovery planning and testing, privileged access controls, multifactor authentication, proactive scanning and testing, and an overall incident response readiness, among other requirements. It is therefore critical to carefully prepare the underwriting submission to the insurers if a company wants to maintain or access insurance coverage. Companies should be conscious that they will need to implement additional safeguards if they are not a first-class risk, and adapt their cyber risk management to evolving threats. Insurers will only accept well-managed, secured risks.

Q. Going forward, do you expect cyber risk management will continue to climb the boardroom agenda as a major issue?

A. Risk managers have increased their awareness of the economic and reputational impact that a critical incident can have on their business. This is translating into a higher demand for cyber insurance and we see that for most large companies, cyber security is one of the top risks that boards address. Companies that delay in addressing cyber security should be aware that the evolving environment, both in terms of security threats and regulation, will lead to more claims against companies and their boards. Additionally, companies will have to demonstrate to investors that their environmental, social and corporate governance (ESG) footprint and performance, to which both cyber security and governance criteria are very relevant, are aligned with their investors' sustainable financial and values objectives. ❑

www.aon.com

AON PLC is a leading global professional services firm providing a broad range of risk, retirement and health solutions. The company's 50,000 employees in 120 countries empower results for clients by using proprietary data and analytics to deliver insights that reduce volatility and improve performance.

CLAUDIA GÓMEZ Executive Director
+34 618 686 525
claudiabeatriz.gomez@aon.es

PABLO MONTOLIU ZUNZUNEGUI Chief Information & Innovation Officer
+34 649 176 891
pablo.montoliu@aon.es

FERNANDO CABALLERO DE LA SEN
Managing Director Global Risk Consulting
+34 91 340 50 00
fernando.caballero@aon.es

AON
Empower Results®

HONG KONG

Protiviti Hong Kong Co Limited

Respondents

MICHAEL PANG
Managing Director
Protiviti Hong Kong Co Limited
+852 2238 0438
michael.pang@protiviti.com

Michael Pang is the practice leader of Protiviti Hong Kong's Technology Consulting and Digital Transformation solutions. He is also the leader of Protiviti's APAC Security & Privacy practice. He possesses 25 years of experience in advising top management on various strategic topics, including cyber security, data privacy protection, IT strategy, IT organisation transformation, IT risk, post-merger integration and operation improvement. He has given many public speeches at industry conferences as well as lectures on cyber security and technology risk topics. Before joining Protiviti, he took key consulting roles at Boston Consulting Group, A.T. Kearney and Kodak Services for Business.

FRANKLIN YEUNG
Director
Protiviti Hong Kong Co Limited
+852 2238 0433
franklin.yeung@protiviti.com

Franklin Yeung is leader of Protiviti Hong Kong's Security & Privacy practice. He has over 21 years of experience in technology consulting, audit and system implementation. He has significant experience in delivering solutions and helping organisations to build up cyber and information security, strategy and governance, risk management and internal control, business continuity management, system implementation and IT project management.

Protiviti Hong Kong Co Limited

Q. How would you summarise today's cyber risk environment? What new risks have emerged in the past 12-18 months?

A. The cyber risk environment in Hong Kong has been getting more dangerous over the past 12 to 18 months. Like the rest of the world, Hong Kong is seeing a significant increase in phishing and ransomware attacks. This increase is likely a result of the sudden need for remote working in response to the coronavirus (COVID-19) pandemic. Since February 2020, the working arrangements for many people have changed. Many individuals who were never required to use laptops or VPNs are now using them daily. Thus, many organisations whose infrastructure was not designed for remote working technologies have been forced to support technologies like cloud computing, VPNs and videoconferencing and collaboration tools. In the 'new normal', IT departments might be asked by management to grant system or data access to an employee's personal device temporarily if the organisation does not have sufficient company equipment to address sudden business demands. This has also increased cyber security risk exposures for organisations. These developments create a lot of new vulnerabilities and attack surfaces for hackers. Ransomware attacks have provided companies with new challenges. In responding to ransomware attacks, a company's data backup strategy, security and availability becomes very important.

Q. What demands are data privacy laws placing on companies in Hong Kong to implement security measures and follow notification requirements? How challenging is it to maintain regulatory compliance?

A. Hong Kong's privacy regulations, the Personal Data (Privacy) Ordinance (PDPO) was established in 1996. The PDPO provides a set of high-level requirements on privacy management, but it lacks a few key elements, such as mandatory data breach notification. It also includes relatively weak penalty clauses for data breaches and inadequate regulatory powers to investigate and prosecute. Unlike Singapore and other Asia-Pacific countries, Hong Kong currently has no 'cyber security law', not even for critical infrastructure organisations. Under the current regulatory environment, it is very easy to maintain regulatory compliance without any strict cyber security or privacy laws.

Q. Would it be fair to say that, in general, organisations are still not up to speed on detecting security breaches and privacy risks quickly enough?

A. From our experience, many organisations in Hong Kong are still not up to scratch in terms of identifying and detecting security breaches and privacy incidents. The primary factor in this assessment is that many companies still do not put enough effort into establishing a set of good cyber security policies and a dedicated cyber security team. Many companies still believe cyber security can be handled on a part-time basis by an engineer in the IT team, however cyber security should never be a part-time job. Furthermore, we often see a significant increase in maturity levels when companies start to establish a dedicated cyber security team. The second factor is that most cyber security teams are simply focused on protecting data and systems, while monitoring and responding are

> *Many companies still believe cyber security can be handled on a part-time basis by an engineer in the IT team, however cyber security should never be a part-time job.*

Protiviti Hong Kong Co Limited

treated as secondary concerns. Another factor is some cyber security teams are too reactive in only trying to patch known vulnerabilities, rather than proactively looking at unknown vulnerabilities, signs of breaches, exploitation or suspicious activities. Some companies simply do not have the tools and capabilities to collect, gather and analyse logs from all servers and equipment to proactively detect an incident. Even for those companies with sufficient funding and equipped with adequate security tools, the tools might not be deployed appropriately, or their configuration or detection rules might not be aligned such that overall preventive and detective capabilities are enhanced. Some organisations need help to revise the configuration design from time to time. In terms of privacy risks, excessive personal data might still be collected without careful consideration by some organisations to justify their business needs.

Q. What steps should companies take to establish appropriate processes and policies to manage cyber-related risks and keep systems safe?

A. The first step is to establish the baseline of the current cyber security maturity. Second, companies must determine the target cyber security maturity, which depends on their business operations and applicable regulations, as well as the risk appetite. The third step is to establish a roadmap that improves the maturity of cyber security management. The final step is to ensure the security controls are properly designed, tested, monitored and calibrated to utilise their ultimate capabilities from time to time. Cyber security processes and policies should not simply focus on protection.

Q. How are insurance providers enhancing their cyber insurance solutions to meet market demands and help companies manage the downside?

A. Traditional cyber insurance solutions are a fixed premium product. And the solutions often just provide financial loss coverage for companies. However, as the insured face increasing threats in terms of complexity and severity, insurance providers must provide more comprehensive support to companies. Such support will also ultimately reduce

Protiviti Hong Kong Co Limited

the exposure of the insurance providers. Normally, insurance providers will ask insureds to fill in self-assessment questionnaires about their current cyber security maturities. The level of maturity certainly affects the insurance providers' risk exposure and hence the premium. Some providers are now offering additional consulting and advisory support for insureds to increase companies' cyber security protection. Apart from compensating for companies' financial loss, some insurance providers also provide a range of post-incident support, such as public relations and communication, legal advisory and incident forensics. This much-needed support could help companies contain an incident and its associated damage and loss.

Q. What considerations should companies make when evaluating cyber insurance coverage, including pricing, policy provisions and exclusions?

A. Companies should know what insurance product or coverage is fit for their business units or organisation by matching their cyber security risk profile and risk appetite. Companies should review their cyber security risk management capabilities and implement necessary security controls before looking for insurance providers to add another layer of support. Companies would be advised to not simply transfer their cyber security risk to any insurance provider without doing any risk mitigation. Brand name and premium cost should not be the key factors in determining the right insurance provider. Product and coverage matching should be carefully considered. Some insurance providers might offer pre-loss or post-loss service support to insureds. Thus, companies should review whether these services would benefit their cyber security risk management.

Q. Going forward, do you expect cyber risk management will continue to climb the boardroom agenda as a major issue?

A. It is only a matter of time before cyber risk becomes one of the major issues on the boardroom agenda. However, we see a general lack of awareness of cyber issues among C-suites executives, except for the chief information officer (CIO) and chief information security officer

(CISO), and board of directors in most companies. Senior executives and directors in more traditional industries, such as manufacturing and retail, still see cyber risk management as being optional, and thus give it lower priority than other issues, such as marketing, business development and sales. It is not unheard of for some companies that have already experienced cyber security incidents to decide not to put in place the sources and investment required to improve their cyber security processes and practices. Often the problem is not only due to a lack of awareness, but also a lack of motivation. ❑

www.protiviti.com

PROTIVITI is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. The firm's consulting solutions span critical business problems in technology, business process, analytics, risk, compliance, transactions and internal audit. Protiviti is committed to attracting and developing a diverse workforce of professionals who share the common value of collaboration. As an organisation, the firm believes that by working with its clients, it can see beyond the surface of changes and problems organisations face to discover opportunities others might miss and face the future with greater confidence.

MICHAEL PANG Managing Director
+852 2238 0438
michael.pang@protiviti.com

FRANKLIN YEUNG Director
+852 2238 0433
franklin.yeung@protiviti.com

protiviti

FINANCIER
WORLDWIDE corporatefinanceintelligence

INDEPTH FEATURE

CYBER SECURITY & RISK MANAGEMENT

2022

FINANCIER WORLDWIDE corporatefinanceintelligence