Guidehouse

Published by Financier Worldwide Ltd

INDEPTH FEATURE Reprint July 2020

CYBER SECURITY & RISK MANAGEMENT

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

UNITED STATES

Guidehouse

Respondents

MARIANNE BAILEY
Director
Guidehouse
mbailey@guidehouse.com

Marianne Bailey leads Guidehouse's advanced solutions cyber security practice. Leveraging Guidehouse's expertise in strategy and security architectures, cyber resilience, chief information security officer (CISO) support, incident prevention and response, identity and access management (IAM), high value asset management, and data and privacy protection she partners with clients to develop and sustain solutions to mitigate cyber security risks against current and emerging threats. She has over 35 years in government, leading US cyber security organisations and driving emerging cyber initiatives for the nation and its allies.

DONALD HECKMAN
Director
Guidehouse
dheckman@guidehouse.com

Donald Heckman leads the Guidehouse cyber security, data protection and privacy capability offerings for public and commercial sector clients, as well as developing and leading a strong cyber security offering for commercial financial sector clients. He has over 36 years of experience in government leadership, spear-heading cyber security and secure information sharing initiatives across the Department of Defence (DoD) and national security sectors. Most recently, he served as both principal deputy for cyber security and deputy chief information security officer (DCISO) at the DoD chief information office (DOD CIO).

Guidehouse

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 for most organisations is becoming more complex and challenging, with remote operations being driven by the current COVID-19 pandemic and the addition of new technologies like 5G, the internet of things (IoT), and the medical IoT (MIoT). These new technologies expand the attack surface of enterprise IT for organisations at an exponentially increasing pace, making it difficult for cyber security teams to protect organisations. With an uncertain global economic outlook for most countries, cyber criminals will increasingly target financial institutions and expand their activities in other sectors, including healthcare, energy and transportation. Phishing and ransomware attacks continue to be successful and are expected to become even more sophisticated as they employ automation and artificial intelligence (AI). Data and privacy breaches will continue to be a major issue despite the increased legislation and regulations, public scrutiny and C-suite focus.

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: Currently in the US there is no central, federal privacy law like the EU's General Data Protection Regulation (GDPR). However, there are several federal privacy laws such as the Privacy Act of 1974, as well as a new generation of consumer-oriented privacy laws coming from multiple states, most notably the California Consumer Privacy Act (CCPA), which constitutes the broadest and most comprehensive privacy law in the US to date. The CCPA imposes significant demands on cyber security and data privacy teams for protecting and maintaining personal data, ensuring its accuracy and significantly reducing times for breach reporting. It is very challenging to maintain regulatory compliance for multiple varying standards with respect to customer privacy and data protection. A

Guidehouse

recent International Association of Privacy Professionals study found 43 percent of organisations are currently working to comply with two to five data privacy laws. This leads to significant complexity, operational cost and process inefficiencies as companies try to design and implement data protection and privacy programmes.

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: Consistent with recent studies, a 2019 IBM-Ponemon Institute study found it took organisations over 200 days to identify a breach, on average, and they spent over $3m on breach costs. These averages will only get worse as advanced persistent threat actors become more sophisticated. Compounded by the significant increase in the number of smart devices enabled by 5G and the IoT, non-harmonised cyber security and privacy regulations, and the expansion of remote operations driven by the COVID-19 pandemic, organisations' cyber security resources, both human and financial, have been stretched very thin. These factors are driving organisations to implement more mature incident response programmes utilising automated detection and response capabilities.

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

A: There are foundational cyber security practices that every organisation should implement to manage cyber-related risk. First, companies must know their environment. You cannot protect what you do not know needs protecting. Identify your high-value assets, data and devices. Second, make sure every device is configured correctly and up to date on security patches. Patch promptly when new patches are released. Third, utilise strong multifactor authentication for every user on the system and implement least-privileged principles. Monitor and audit privileged users using a privileged access management system. Fourth, implement a strong vulnerability management programme with regular scanning and remediation. Fifth, create robust incident response and business continuity plans based on privacy and business impact

Guidehouse

assessments and exercise them regularly. Finally, participate in cyber security threat intelligence sharing and adjust corporate preventive controls based on current threats.

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

A: Insurance providers offering cyber insurance are just getting started. To date, insurance is focused on legal costs and identity protection. Some of the challenges they are facing in providing cyber insurance are related to the uncertainty around pricing and claims provisions due to lack of historical data. Additionally, they are not able to predict the new risk arising from emerging technologies and to determine or quantify the monetary impacts. And last but certainly not least, the threat that insurers are most worried about remains a catastrophic cyber event that could cause extensive losses, leading the insurance provider to insolvency. Ultimately, it is hard to place a dollar value on the reputational damage and costs due to lost consumer confidence done by

Companies must know their environment. You cannot protect what you do not know needs protecting. Identify your high-value assets, data and devices.

Guidehouse

some of the more recent high-profile cyber attacks and data breaches.

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

A: There are two primary cyber insurance coverage considerations, legal fees and expenses for impacted customers, and business impact fees and lost revenues, that companies should evaluate. The first is errors and omissions (E&O) coverage, which includes negligence or breach of contractual obligations due to cyber incidents, and indemnification legal defence costs resulting from a lawsuit or dispute with customers or the public at large. The second is network security coverage in the event of business systems failure due to ransomware, malware, insider threats, employee negligence or third-party data breaches. Both are equally important, but the E&O coverage tends to get the most focus due to the high-profile media coverage of impacted customers.

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

A: Given the significant increase in high-profile breaches globally, boards of directors are acutely aware of cyber risks. These cyber incidents have the potential to directly impact a company's finances, through loss of market share and consumer trust, reputational impact, and legal and regulatory costs. Most organisations now realise that cyber security is not just the job of the chief information security officer but the entire C-suite. As data protection and privacy laws and regulations continue to expand, chief privacy officers and chief data officers are being added to the board and are gaining more influence. A NewVantage Partners 2019 research report shows that more than 67 percent of large companies now have a chief data officer on their board. There is a growing trend across organisations to integrate their cyber security and privacy teams to more effectively and efficiently address

these new data protection and privacy regulations. ❑

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 scalable, innovative solutions that prepare them for future growth and success. Headquartered in Washington, DC, the company has more than 7000 professionals in more than 50 locations. Guidehouse is a Veritas Capital portfolio company.

MARIANNE BAILEY Director
mbailey@guidehouse.com

DONALD HECKMAN Director
dheckman@guidehouse.com