Guidehouse

Published by Financier Worldwide Ltd

INDEPTH FEATURE Reprint April 2021

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
Partner
Guidehouse
mbailey@guidehousefederal.com

Marianne Bailey is a partner at Guidehouse who leads the advanced solutions cyber security practice to provide strategies and solutions which enable Guidehouse clients to manage their cyber security risks. Ms Bailey brings over 35 years of experience across the Department of Defense (DoD), intelligence community, and civil government sectors. She served as deputy national manager for National Security Systems (NSS) and senior cybersecurity executive for the National Security Agency (NSA) where she was directly responsible for systems across the government containing classified or sensitive information.

DONALD R. HECKMAN JR.
Director
Guidehouse
dheckman@guidehousefederal.com

Donald Heckman, a cyber security subject matter expert, is a director in Guidehouse's advanced solutions. He is the defence cyber solutions leader developing and leading strong cyber security offerings for defence sector clients, as well as clients in financial services, healthcare, energy, national security and state and local governments. He works with Guidehouse 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, secure information sharing and data protection.

REPRINT

Guidehouse

Q. In your opinion, what are the major cyber threats to which today's companies are vulnerable?

A: When it comes to the technology exploited and the means of exploitation, the technical threats today are not much different than what we have seen over the past few years. The cyber trade craft is pretty much the same and includes gaining access to the network or to your applications through poor identity and access control mechanisms, scanning the internal network to look for unpatched systems, out-of-the-box passwords still being used, poor system admin passwords and so on. What is different is that companies are beginning to see the true impact of a cyber attack, and it reaches well beyond the IT department. It is all about business, mission and resiliency. When it comes to cyber today, companies should be talking cyber resilience: critical systems, crown jewels, high value assets, keys to the kingdom, whatever systems support their primary business functions, and every system and person that has access to them. Companies need to act now to understand how an adversary could exploit their business functions through cyber actions by attacking those crown jewels.

Q. Given the risks, do you believe companies in the US are placing enough importance on cyber security? Are board members taking a proactive, hands-on approach to improving policies and processes?

A: Cyber security is an evolutionary process and companies tend to spend what they feel they must to manage the risk of doing business in this globally connected digital world. Board members realise there is significant risk and they are constantly upping their game to address that risk. Most companies or organisations do not understand or appreciate the extent of their risk from a cyber attack. Very few have taken a hard look at what is required for their company to become cyber resilient. Today, regulations are the primary mechanism driving focus in this area.

Q. To what extent have cyber security and data privacy regulations changed in the US? How is this affecting the

Guidehouse

way companies manage and maintain compliance?

A: US cyber security and privacy regulations continue to be of focus across individual states, as well as the federal government. California voters passed the California Privacy Rights Act, which will significantly alter the state's current law when fully enacted in 2022. Currently, at least 11 other states are considering privacy-related legislation in 2021. Federal privacy and cyber security legislation is expected to regain focus under the Biden administration, due to the EU-US Privacy Shield invalidation last year and the recent SolarWinds hack. Given that the US does not have a uniform federal regulation for either privacy or cyber security, companies that do business in the US must understand and demonstrate compliance in each state they operate in. It can be a challenge to remain compliant, as these regulations are rapidly evolving and sometimes contradict each other.

Q. In your experience, what steps should companies take to avoid potential cyber breaches – either from external hackers or internal sources such as rogue employees?

A: To avoid potential cyber breaches, companies should have a documented comprehensive cyber security programme that includes people, technology and operations. They should implement cyber security best practices and promote a culture where cyber security is everyone's responsibility. Some best practices that have the most impact for preventing breaches include ensuring you know what assets are in your environment, and that they are configured securely and patched with the most up-to-date software. Companies should strongly authenticate every user with multifactor authentication and allow users access only to what they need to do their jobs. Users, especially privileged users, should be monitored for abnormal behaviour. And finally, companies should have a robust training programme for every employee, since more than 90 percent of breaches are caused by human error.

Q. How should firms respond immediately after falling victim to cyber crime, to demonstrate that they have done the right thing in the event of a cyber breach or data loss?

Guidehouse

A: Every firm should develop and exercise an incident response plan. Figuring out what to do in the middle of a breach is unacceptable in today's cyber and regulatory world. Companies must activate their incident response plan. They must also contact their office of general counsel (OGC) to determine reporting obligations, based on the specific details of the event. A further important step is to turn on logging for high-value assets if it is not enabled and start collecting data. Companies should also collect network traffic flow logs and isolate compromised endpoints from the network and begin rebuilding clean and secure versions of the endpoints. Before resuming production, companies should test rebuilt endpoints to ensure they are clean and secure and perform forensic analysis of the endpoints that have been or may have been compromised. Compromised user account passwords must also be changed, which may require all users to change their account passwords, depending on the severity of the incident. Finally, companies must also update outbound firewall rules to block unusual traffic and remind employees about safe email and web-browsing practices.

Every firm should develop and exercise an incident response plan. Figuring out what to do in the middle of a breach is unacceptable in today's cyber and regulatory world.

Guidehouse

Q. In what ways can risk transfer and insurance help companies and their directors and officers to deal with cyber risk, potential losses, and related liabilities?

A: Cyber security insurance is designed to protect insured companies against losses resulting from cyber incidents. Most of these policies require the insured companies to implement cyber security best practices and adopt preventive measures to obtain either increased coverage or better rates. These safeguards can improve overall cyber risk management for the insured companies. That said, we would caution companies to not be too reliant on insurance or just implementing the minimum standards. They should be continually looking to improve their cyber security programme. While insurance can potentially shield your company from financial losses, it cannot protect the impact to your company brand from the loss of customer trust resulting from an incident.

Q. What are your predictions for cyber crime and data security in the US over the coming years?

A: Cyber crime will continue to evolve, expand and become more sophisticated, which will drive an increase in data security regulations, technologies and professionals across the US and around the world. As a result of the pandemic and the rapid adoption of remote work environments, the attack surface of many companies has greatly expanded, creating new opportunities for cyber criminals. The number of cyber attacks in 2020 were significantly greater than the previous year and continued to evolve and become more sophisticated. As cyber security teams try to make use of artificial intelligence and machine learning for cyber defence, so do the attackers. Sophisticated advanced persistent threat actors will probably take a more hands-on approach to their attacks to strategically insert and manoeuvre to avoid detection. Attacks will continue to be successful, which will increase the calls for legislation and regulation and could drive the US to adopt a uniform federal privacy law. These attacks will highlight the need for improved data

Guidehouse

protection strategies and drive adoption of data security technologies. Finally, the demand for data protection and privacy professionals will continue to grow, and supply will not keep up with demand for these individuals. ❑

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.

MARIANNE BAILEY Partner
mbailey@guidehousefederal.com

DONALD R. HECKMAN JR. Director
dheckman@guidehousefederal.com