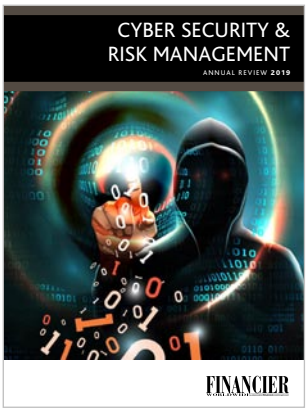

NAVIGANT

Published by Financier Worldwide Ltd

ANNUAL REVIEW Reprint July 2019

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

JOSEPH S. CAMPBELL
Navigant Consulting, Inc.
Director
+1 (202) 384 8199
joseph.campbell@navigant.com

Joseph Campbell is a director in Navigant's Global Investigations & Compliance practice. His role involves leading anti-bribery and corruption, anti-money laundering (AML) and financial investigations. Mr Campbell's experience includes investigation and assessment of cross-border tax matters through review and analysis of business and financial institution international investments and transactions. Prior to Navigant, he worked at the Federal Bureau of Investigation (FBI) for more than 25 years. He was the Assistant Director of the Criminal Investigative Division, responsible for a team of 6000 special agents, analysts and forensic accountants.

Q. In your opinion, what are the major cyber threats to which today's companies are vulnerable? Could you comment on any recent, high profile cyber attacks in the US?

CAMPBELL: Information security breaches have significant consequences for businesses. Major cyber threats include ransomware, spearphishing, business email compromise, malware and insider malfeasance. While no business is immune to cyber threats, often affected industries include public works and infrastructure, energy, healthcare and financial services. In 2015, the US Office of Personnel Management experienced a cyber penetration that impacted over 21 million people and exposed serious counterintelligence vulnerability for the US government. Other noteworthy data breaches affecting hundreds of millions of consumers have hit Marriott Starwood Hotels, where sensitive passport information was compromised, as well as Quora, Google, Anthem and T-Mobile.

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

CAMPBELL: The proliferation of breaches is spurring board members to become more involved in cyber security prevention and get involved in reviewing cyber security incident response plans and participating in breach exercises. Boards understand that simply spending money on purchasing IT protection is inadequate. For this reason, it is important to consider adaptive technologies and teams, as well as data governance strategies to reduce attack targets. Best practices for companies arming themselves against cyber security threats include incorporating accepted international standards, such as the National Institute of Standards and Technology Cybersecurity Framework and the International Organization for Standardization 27001 framework.

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

CAMPBELL: The Financial Crimes Enforcement Network provided guidance concerning cyber security relative to 'Suspicious Activity Report' requirements under the Bank Secrecy Act, and the New York State Department of Financial Services issued cyber security regulations for covered entities. With increased regulation and reporting requirements, companies are developing a culture of data compliance with policies and procedures, and companywide training for compliance with new laws, such as the breach notification laws that now exist in all 50 states. At least 35 states have also enacted data disposal laws, and California is the first state to pass a specific consumer privacy law. Others are considering similar legislation.

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

CAMPBELL: Companies must understand their technology vulnerabilities and risks, and design systems and processes for risk mitigation. They should consider working with a reputable digital forensics entity, and incorporate a plan such as the Seven Pillars of Cyber Resilience, which includes strong corporate governance around cyber security policies and procedures, knowing their data, value and protections, testing of

security systems, awareness of cyber security systems information and guidelines, designation of specific persons to implement cyber security, preparation to immediately implement an incident management plan upon attack, and having a plan to recover and adapt lessons learned.

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?

CAMPBELL: After detecting and verifying a security breach, organisations should investigate and assess the circumstances of the event, contain the impact and secure their systems. The goal is to limit the effects of the incident. Organisations should report the incident to appropriate individuals and government agencies and alert employees and the public of the event. Recovery efforts should include restoring and rebuilding systems and updated patching. An organisation should conduct remediation efforts and a root-cause analysis, followed by implementation of vulnerability mitigation. Lessons learned should be reviewed with improvement of training and use of appropriate security controls and protocols.

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

CAMPBELL: Purchase of cyber security insurance is rising and can help companies transfer loss in the event of a cyber security breach. Coverage can assist companies by promoting the adoption of preventive measures in return for increased coverage, and basing premiums on an insured's level of self-protection, thereby encouraging the implementation of best practices. Coverage may also require companies to use certain vendors for breach response and recovery. Coverage does not relieve companies of their obligation to comply with applicable breach incident reporting regulations, nor will it help them avoid managing the breach response and resulting reputational damage.

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

CAMPBELL: Maintaining the privacy and security of data continues to be a challenge for companies balancing the use of personal information for productive business processes with protecting customers and complying with privacy-related laws. To avoid problems down

"Companies should educate themselves on applicable data security and privacy laws, and develop underlying data and cyber security governance and strategy."

the road, companies should educate themselves on applicable data security and privacy laws, and develop underlying data and cyber security governance and strategy. This should be a companywide effort, and organisations should be sure they have the right team in place, assign clear roles and responsibilities, conduct training, and move quickly in the implementation of their data security and privacy plans. ■

www.navigant.com

NAVIGANT

Navigant Consulting, Inc. is a specialised, global professional services firm that helps clients take control of their future. Navigant's professionals apply deep industry knowledge, substantive technical expertise, and an enterprising approach to help clients build, manage and protect their business interests. With a focus on markets and clients facing transformational change and significant regulatory or legal pressures, the firm primarily serves clients in the healthcare, energy and financial services industries. Across a range of advisory, consulting, outsourcing, data security and privacy, and technology and analytics services, Navigant's practitioners bring sharp insight that pinpoints opportunities and delivers powerful results.

JOSEPH S. CAMPBELL
Director
+1 (202) 384 8199
joseph.campbell@navigant.com