REPRINT FINANCIERWORLDWIDE.COM

ANNUAL REVIEW

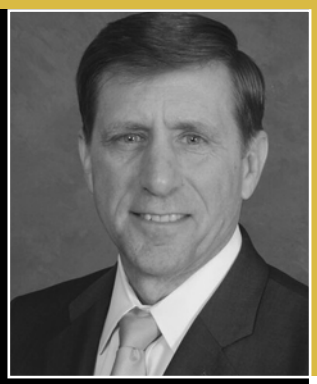
Cyber security & risk management

REPRINTED FROM
ONLINE CONTENT
JULY 2018

PREPARED ON BEHALF OF

MARSH

FINANCIER WORLDWIDE corporatefinanceintelligence



THOMAS FUHRMAN
Marsh Risk Consulting
Managing Director, Cybersecurity Consulting and Advisory Services
+1 (202) 263 7827
thomas.fuhrman@marsh.com

Thomas Fuhrman is managing director, cybersecurity consulting and advisory services, at Marsh Risk Consulting (MRC). He leads MRC's cyber risk consulting practice in North America and in international markets and works across Marsh & McLennan's operating companies on a broad range of cyber initiatives. He is an experienced cyber security consultant with over 20 years in the business. He was an active contributor to the development of the NIST Cybersecurity Framework and has advised clients and boards on its implementation. He is a strong advocate of the strategic management of cyber risk at the enterprise level through cyber risk quantification.

United States

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

FUHRMAN: Today's cyber risks arise from the shared reliance on ubiquitous and vulnerable technologies. In the past several years, cyber attacks have become more sophisticated, more destructive and more common. Some of this sophistication comes from the availability of attack techniques and methods, which reportedly originated from sources, such as nation-state military intelligence and services and advanced cyber crime syndicates. The 'WannaCry' ransomware attacks and the destructive 'NotPetya' attacks of 2017 are prime examples, and we expect many more. NotPetya, which disabled and effectively destroyed large numbers of servers and desktop computers worldwide, was disastrous for two reasons. First, it targeted specific un-patched configurations of Windows's operating systems. Second, the malware code was aggressively self-propagating and designed to disable functioning systems. Once inside a network, it rapidly installed itself in all the machines it could find. These two characteristics will likely be part of many future cyber events.

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

FUHRMAN: The European Union's General Data Protection Regulation (GDPR) requires all firms, including US ones, holding data on persons in Europe to establish more effective data governance policies and procedures in relation to data classification, storage, protection and lifecycle management. A major GDPR challenge for companies is implementing the data rights it defines, including the consumer's right to access one's data, to be forgotten and to data portability.In many cases, technology transformations are needed to provide the functionality these rights imply. Articles 25 and 32 to 34 outline data protection requirements, and Article 42 encourages the establishment of "data protection certification mechanisms" issued by certification bodies. These provisions may present substantial cyber security requirements. GDPR is seen as the harbinger of data protection regimes to be implemented in the US and beyond. Already, every US state has data breach laws governing disclosure and other requirements, which often intersect with GDPR's requirements. We should anticipate a convergence over time of legal requirements for personal information protection and data owners' rights, likely at the US federal level.

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?

FUHRMAN: Today's detection technology requires intricate setup and integration, as well as trained operators to configure, manage, monitor and react to its alerts. Finding qualified cyber security professional staff to do this work is a major challenge unto itself. Additionally, the frequency of false positives sends analysts down blind alleys and distracts them from analysing true threats. This is a key area in cyber security where artificial intelligence (AI) and automation may reduce time consuming and error prone cyber event analysis by human operators. Various kinds of machine learning are in place in today's cyber sensors and analytical platforms, but this is just the beginning. Systems like these need to grow in capability and sophistication to not only relieve the burden of human operators, but also improve real-time automated analysis and responses to cyber alerts and anomalies. Hackers are using AI; defenders need to do the same.

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

FUHRMAN: Companies should adopt a structured approach to cyber security governance. That means establishing the structure for decision making in cyber security, identifying compliance requirements, defining and aligning roles, responsibilities and organisations for managing cyber risk; selecting a cyber programme development framework, such as the NIST Cybersecurity Framework or ISO 27000 and defining the process linkage between key stakeholders and operations for the identification, measurement and management of cyber risk. With these elements in place, it is then time to review, refresh or create enterprise

IT and cyber security policy documentation. This may focus on enterprise-wide cyber security, employee cyber security responsibilities, awareness and IT acceptable use, identity and access management, data classification, cyber risk management, third-party or vendor management, incident response and escalation, and mobile device security. Once the governance and policy frameworks are designed, an integrated set of operational procedures should be developed.

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

FUHRMAN: The biggest change in insurance has been the shift in buyers' focus from coverage for data and privacy breaches to business interruption (BI) and contingent business interruption (CBI) risks – especially economic losses caused by operational, system and supply chain disruptions. With many non-traditional buyers of cyber insurance, including manufacturing, energy and pharmaceutical companies, increasingly seeking BI coverage, underwriters are responding with broader terms and higher limits. New market entrants are keeping pricing competitive while increasing overall capacity. Key BI innovations include CBI and supply chain coverage, coverage triggers beyond security breaches and coverage that responds to losses incurred from the start of waiting periods. Insurers are also focusing on tailoring coverage to small and medium size firms' needs and simplifying the underwriting process. Finally, insurers continue to provide services aimed at improving policyholders' risk profile, such as cyber risk education programmes and risk mitigation tools that assist with prevention and recovery from cyber attacks.

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

FUHRMAN: While pricing is always a factor in purchasing insurance, it should be secondary to obtaining the appropriate breadth of coverage. Companies should work with a qualified broker to better understand their cyber risk profile, evaluate marketplace offerings and design an optimal insurance programme. The first step is an accurate assessment of the company's cyber risks. What are the external and internal vulnerabilities, and how susceptible is the firm to cyber attack? Secondly, what would a cyber event cost the company? Quantifying cyber risk is critical for driving informed decision making around cyber security investment and risk transfer planning. Another consideration is risk appetite; how much risk is the firm willing and able to bear? These metrics help determine the company's cyber insurance needs. A broker can model maximum potential losses and analyse the firm's current risk transfer portfolio to evaluate policies and limits, identify gaps, overlaps or coverage needs, and design a coverage solution.

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

FUHRMAN: Cyber is one of the greatest risks that organisations face and management of this risk is essential. Boards know this and are increasingly aware of their fiduciary and risk

"While pricing is always a factor in purchasing insurance, it should be secondary to obtaining the appropriate breadth of coverage."

oversight responsibilities. Additionally, the Securities and Exchange Commission (SEC) recently released guidance on understanding and disclosing business-material cyber risks to investors. This is a board-level issue. A clear link, through policy and process, between board, management, IT and cyber security functional teams, is needed to ensure effective management of this critical risk. In cyber security, we use the acronym 'APT' to refer to advanced persistent threat malware. I suggest another meaning for that acronym, 'accountability for precision and transparency' in the enterprise management of cyber risk. That means understanding the risk, in financial terms, and managing it through closed loop processes to achieve business goals. This should be an ongoing pursuit for all organisations that depend on IT systems. ■

www.marsh.com

MARSH

THOMAS FUHRMAN
Managing Director, Cybersecurity Consulting and Advisory Services
+1 (202) 263 7827
thomas.fuhrman@marsh.com

JIM HOLTZCLAW
Senior Vice President
+1 (202) 297 9351
james.holtzclaw@marsh.com

THOMAS REAGAN
Cyber Practice Leader
+1 (212) 345 9452
thomas.reagan@marsh.com

Marsh is a global leader in insurance broking and innovative risk management strategies with 30,000 employees advising individual and commercial clients of all sizes in over 130 countries. Marsh's Cyber Centre of Excellence harnesses its cyber risk, brokerage and advisory expertise under one roof to deliver proprietary, purpose-built and market-leading cyber risk management products and solutions to its clients worldwide.