Raising cyber risk to the enterprise level

Cyberattacks are strategic business threats that can impact the financial, reputational and operational viability of an organisation

Board members and C-suite executives, although not typically experts in technology, must take ownership of cyber risk, working in concert with critical organisational stakeholders, such as finance, legal, human resources, risk and information technology/security managers.

This article offers guidance to help top executives and directors understand the escalating nature of cyber risk, their role in overseeing it at the enterprise level, and key questions that pertain to effective cyber risk management.

Elisabeth Case
MD and Head of Client Advisory, Marsh US Cyber Practice

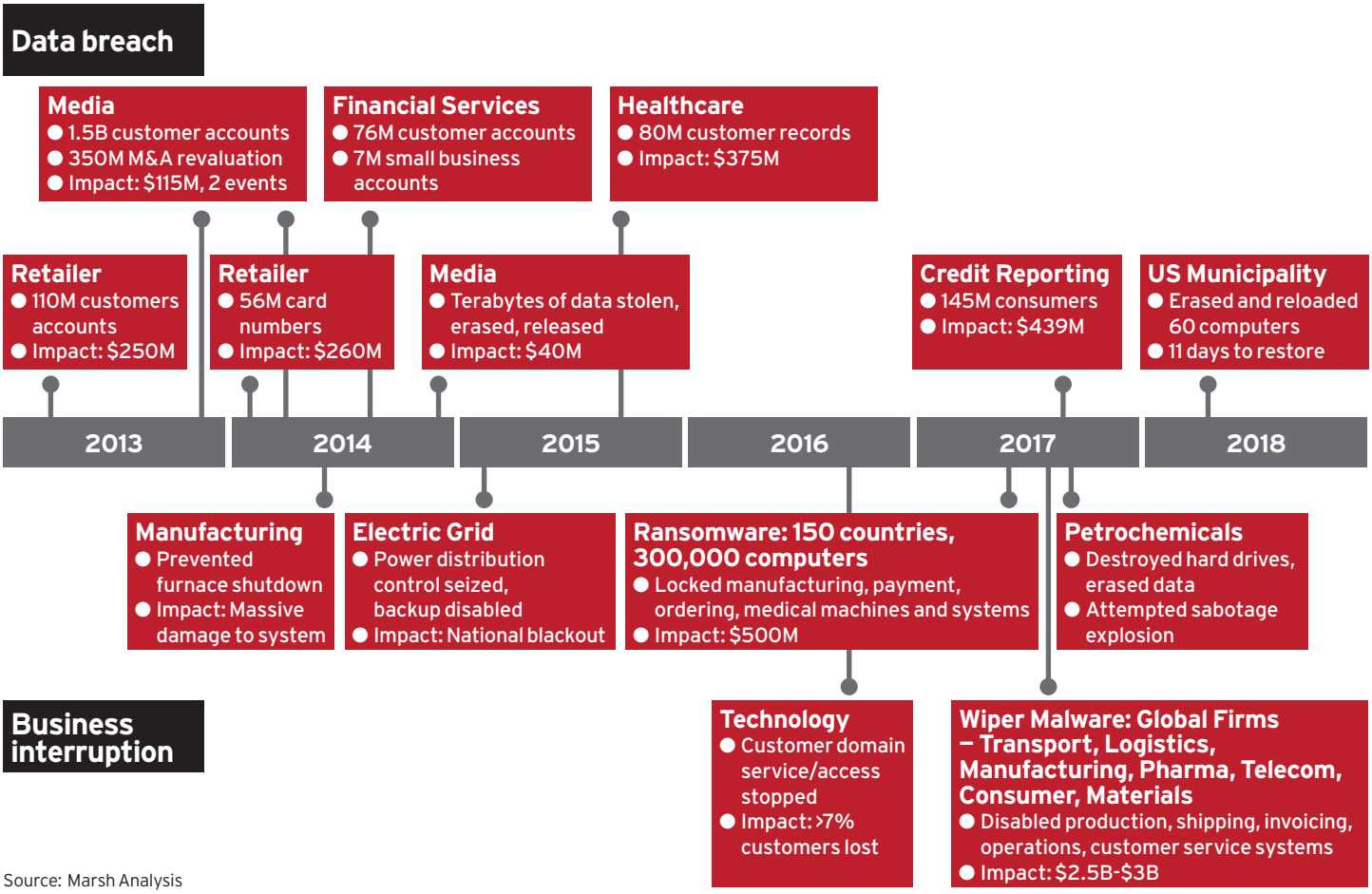
A fast-evolving cyber risk landscape

Cyber threats today have evolved beyond data breach to highly sophisticated schemes designed to disrupt businesses and supply chains, costing organisations billions of dollars. Last year's WannaCry and NotPetya malware attacks were the latest wake-up calls, especially for firms in industries not traditionally targeted by cyber hackers, such as manufacturing, logistics and transportation, among others.

The attacks paralysed global companies for days and inflicted significant economic damage. Supply chain and operational disruption from NotPetya alone caused more than $3billion in economic losses and revenue disruption, spotlighting the economic toll cyberattacks can have on any industry and the interconnectivity of cyber vulnerabilities worldwide (see Figure 1, below).[1]

Even as hackers become more inventive, changes in technology, geopolitics and regulation are increasing cyber exposures and creating new susceptibilities: the accelerating use of the Internet of Things, artificial intelligence and machine learning in business operations; the rise of

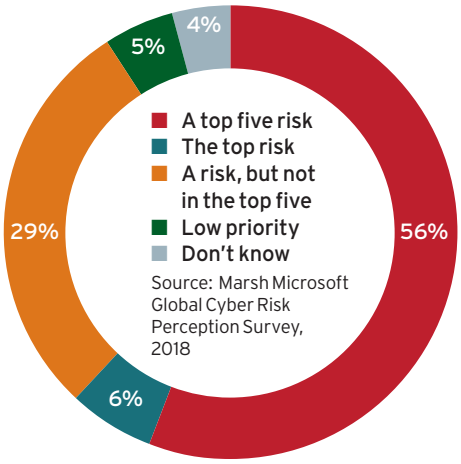
FIG 1: MAJOR CYBERATTACKS, 2013-2018 Impact: Financial losses and expenses (estimated)



Source: Marsh Analysis

FIG 2: MOST ORGANISATIONS NOW RANK CYBERSECURITY AMONG THEIR HIGHEST RISK MANAGEMENT PRIORITIES

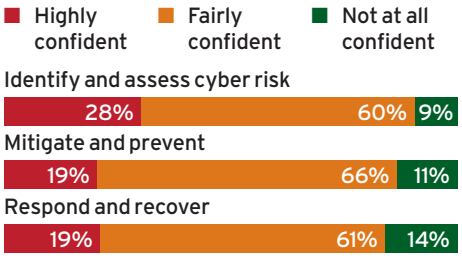
Among my organisation's risk management priorities, cyber risk is:



Source: Marsh Microsoft Global Cyber Risk Perception Survey, 2018

FIG 3: EXECUTIVES ARE MORE CONFIDENT OF ORGANISATIONS' ABILITY TO UNDERSTAND AND ASSESS CYBER RISK THAN OF MITIGATING OR RESPONDING TO IT

Regarding cyber risk, for each of the following, please indicate your confidence in your organisation's ability



Source: Marsh Microsoft Global Cyber Risk Perception Survey, 2018

FIG 4: BOARD MEMBERS NEED MORE INFORMATION REGARDING CYBER RISK MANAGEMENT

There is a disconnect between the information board members say they receive versus what others say they share with them

45% of risk and technology executives said they send information on cyber investment initiatives to board members

...yet only...

18% of directors said they receive such information

nation-state sponsored cyberattacks; and the rise of more stringent privacy regulation all have implications for directors and C-suite officers in terms of enterprise protection and stewardship.

Particularly on the regulatory front, requirements for stronger cyber security, breach notification and data stewardship are being adopted in numerous jurisdictions around the world. The EU's General Data Protection Regulation (GDPR), enacted in May, contains wide-reaching provisions that are revolutionising the global data protection landscape, obliging subject companies to review and enhance their privacy and data protection practices or face significant fines and penalties – as high as €20million or four per cent of global revenue, whichever is higher. China's Cyber Security Law and Australia's Privacy Amendment are other examples of recently enacted sovereign regulations around data security and protections. In the US, the Securities and Exchange Commission recently issued interpretive guidance for public company disclosure of cyber security risks and incidents. And in California, new data privacy legislation established ground-breaking privacy protections for consumers – the first instance of what may be a tide of new state-based consumer privacy legislation.

In this environment, the cyber threat is well recognised: most organisations rank cyber risk among their highest risk management priorities, according to a recent Marsh Microsoft Global Cyber Risk Perception Survey (see Figure 2, above). However, the same survey reveals a disconnect between the magnitude of concern and the certitude that practices and resources being deployed to manage cyber risk are on target: only 19 per cent of corporate executives say they are highly confident in their company's ability to prevent and respond successfully to a cyber event (see Figure 3, above).

Another notable conclusion from the survey is that high quality information about how an organisation is assessing and managing its cyber risk, which is necessary for effective cyber risk management, is generally lacking at the executive level. That gap exists both in the flow of information – the volume and distribution of data to the board level – as well as in the form that information takes – the language used to express and measure cyber risk exposure. Too often, data about a firm's cyber risk and mitigation efforts is communicated across the organisation in technical terminology that can be challenging for non-technical experts. Instead, cyber risk measurement should be framed in economic terms – the lingua franca of business (see Figure 4, above).

A best practices approach: strategic, quantified and resilient

Directors and officers have a duty to manage cyber risk as they do other material risks to the organisation, given its potential economic, operational and regulatory risk for the firm. Best practice for cyber risk management is a comprehensive strategy built upon the three core pillars of strategic governance, risk quantification and resilience planning. »

GETTING A HANDLE ON CYBER RISK
Board members need to take ownership of cybersecurity

As a strategic risk, cyberthreats should be managed at the enterprise level, not delegated to IT or other functional departments. Likewise, cyber risk should be measured and expressed quantitatively to provide an objective assessment of the value at risk and allow for measurement of the return on the firm's cyber investment – and for comprehension by key stakeholders. And, because cyberattacks are an unfortunate but inevitable occurrence for any organisation today that employs technology, response planning and resiliency preparation are critical to minimise business impact, mitigate damage and loss and strengthen organisational recovery.

Strategic, enterprise -level governance

Good corporate governance in the age of cyberattacks means that cyber risk belongs on the boardroom agenda on a regular, if not continual, basis. Cyber risk management falls firmly within directors' and officers' duty to oversee and protect the financial health of the firm. To bridge the knowledge or experience gaps that directors may face with cyber risk, many boards are recruiting professionals with technical cyber expertise as permanent members of the board or as advisors. Others are integrating cyber risk into the board's risk committee, where it is addressed alongside other enterprise risks, such as compliance, legal, operational and reputational risk, and incorporated into the firm's overall risk management framework (see Figure 5, right).

Each organisation will adopt the governance model that best suits its business, risk profile and technology exposures, but all should embrace the fact that cyber risk merits board-level ownership and integration into the roster of critical issues addressed at the highest level of the organisation.

Cyber risk quantification

Too often, organisations assess their cyber risk exposure qualitatively, using 'traffic light' dashboards, general descriptors, or relative rankings. But qualitative cyber risk assessments don't yield meaningful insight into the potential financial cost of cyber events or guidance for decisions about cyber risk investments. In the 2018 Marsh Microsoft Global Cyber Risk Survey, a third of respondents said they had no method for measuring or expressing cyber risk and only 11 per cent use economic quantification. This leaves considerable room for improvement – one that directors should press for. Equally important for directors, regulators in many jurisdictions are now requiring risk-based assessments that compel organisations to evaluate the financial size of cyber exposures as they do other enterprise threats (see Figure 6, right).

Economic quantification enables cyber risk to be measured, expressed and understood in the common language of business and boardrooms. It shifts boardroom conversation of cyber risk from a technical discussion of threat vectors and system vulnerabilities to a data-driven analysis focussed on optimising a firm's cyber capital allocation and reducing its total cost of risk. A quantified measurement of cyber risk also helps inform decision-making around cyber risk investments – technical mitigation and risk transfer – and allows for evaluation of the risk reduction return on investment. With hard numbers in hand, corporate leaders can consider how much to invest in cybersecurity, how much risk to transfer via insurance and how much risk the firm is willing to retain.

Cyber insurance and cybersecurity are complementary, covering two different sides of the risk curve: whereas technical mitigation (cybersecurity) is useful to prevent and reduce the frequency of cyberattacks, risk transfer (cyber insurance) serves to both lessen the severity of cyber losses and bolster recovery and organisational resilience. And, just as cyber risk should not be wholly delegated to the IT department, decisions about cyber insurance purchasing should be coupled with cybersecurity investment decisions, within the firm's overall risk management considerations.

While directors may not need or want to master every detail of their firm's insurance policies, board members should feel comfortable with the company's overall programme coverages and limits as they apply to its unique cyber risk profile. Cyber insurance continues to evolve, both in terms of risk coverage and market capacity, and most organisations, regardless of industry, will be able to obtain comprehensive coverage that dovetails with their other policies as well as policy wording that is adapted to the firm's specific cyber and technology risks.

Most cyber insurers now offer both first- and third-party coverage that protect a firm from a broad array of cyber exposures. Third-party coverage protects a firm from liabilities that arise to third parties from the organisation's use of technology or the third-party data it collects, maintains and uses. First-party cyber coverage has evolved rapidly in response to market demand to now commonly include business interruption, contingent business interruption and extra expense coverage, as well as the more traditional breach response costs such as notification or cyber extortion (see Figure 7, right).

Cyber insurance offers two important ancillary benefits that should also be of interest to corporate directors. One, it opens the door to a full view of the potential economic cost of a cyber event. The process of applying for cyber insurance requires companies to identify assets at risk, threats and vulnerabilities, evaluate cybersecurity controls, and apply modelling tools to calculate potential costs of cyber events. Second, once a policy is in place, the insured gains a partner in its insurer, who can provide access to experts to help with event recovery – forensic accountants, consumer notification services, public relations firms and legal counsel – all critical assets in a firm's cyber event response strategy.

FIGURE 5: LARGE CYBERATTACKS ARE RISK OF MOST CONCERN TO BUSINESS LEADERS

The risk community ranked cyber as the risk most likely to intensify in 2018[1]

Source: [1]Global Risk Report 2018, World Economic Forum Executive Opinion Survey, with Marsh & McLennan Companies

Resilience & recovery planning

Cyberattacks today are 'when,' not 'if', events. Cyber risk cannot be fully eliminated by technology or entirely transferred off the balance sheet – a critical point for directors to recognise in their overall discussions of risk management and the firm's level of risk acceptance.

Given that, every organisation should invest in preparation and planning to build the resilience necessary to recover and rebound quickly from a cyber event. The quality and speed of a firm's response can be the most important indicator of success in recovering from a cyberattack. Preparation and response planning should involve a number of key organisational stakeholders, including directors and C-suite officers, all of whom have roles to play in cyber event response. The steps involved in preparing to manage and respond to cyberattacks are similar to those used in other crisis or business continuity planning: education, awareness, training, testing, evaluation and performance improvement.

From a director's perspective, this may mean staying abreast of major developments in cyber risk, especially as they pertain to firms in the same industry. This can take the form of executive briefings and seminars which not only provide an overview of current cyber threats, but also help directors understand their responsibilities in helping the firm prepare for, mitigate and respond to a cyber event. It can also mean engaging in table top scenarios, crisis management drills and incident response rehearsals.

As with all crisis management preparation, an important part of cyber incident response planning is the assignment and documentation of roles

and responsibilities. In the event of a cyberattack, leaders will need to understand the organisation's obligations to key stakeholders, such as regulators, shareholders and consumers, have confidence that all actors understand and embrace their roles in the response plan, and be sure that the company has ready access to the resources and outside expertise that it will need to respond and recover effectively.

Helping directors ask the right questions

While every organisation should formulate its own plan for managing and responding to cyber risk, there are common factors and considerations that should help shape every firm's cyber risk management strategy. Likewise, there are universal responsibilities and roles expected of directors in all types and sizes of company: board members should lend their support and sponsorship to the development of the cyber risk management strategy and hold stakeholders accountable for fulfilling their parts in its maintenance and execution.

Numerous resources are available to help directors get their heads and hands around cyber risk. Sometimes, however, the most valuable guidance is not providing hard and fast answers, but counsel as to the right questions to ask. Operating on that premise, we offer below a list of key questions that directors and C-suite officers can use to gain insight into cyber risk assessment and measurement, identify factors driving cyber risk investment decisions, and consider how best to oversee and guide the organisation's cyber risk management efforts.

Questions to help **assess and analyse** cyber risk:

- Do we know the real cost of a cyber event on our firm?
- What risks beyond data breach have we assessed?
- Have we calculated the full value of assets – intangible as well as tangible – at risk?
- Have we quantified our business interruption or supply chain disruption cyber risk?
- What process is used internally to identify likely cyber events?
- Which stakeholders are involved in cyber risk assessment and planning?
- What scenario modelling is used to assess potential impacts of cyberattacks?

Questions to guide optimal investment decisions to **secure and insure** against cyber risk:

- How are we optimising our cyber risk investment?
- How robust is our insurance programme, considering the spectrum of potential cyber events (e.g. business interruption, intellectual property theft, revenue loss, privacy liability, reputational damage, or regulatory actions)?
- How do we assess and monitor third-party/vendor cyber risk?
- Do we understand our risk tolerance threshold?
- Knowing that no cybersecurity measures will reduce our risk to zero, how do we strike the right balance between risk mitigation and risk transfer?
- How do we measure risk reduction effectiveness of our cyber risk investment?

Questions to ensure the firm is strengthening its **cyber resilience**:

- How frequently do we test and update our cyber risk management plan?
- What kind of cyber risk training and education does management engage in?
- What programmes do we have to educate and train employees about cyber risk?
- Have we identified external experts and resources to help us manage and respond to a cyberattack? Have we proactively engaged any of them before an event happens?
- Are we planning for evolving regulations around data protection?

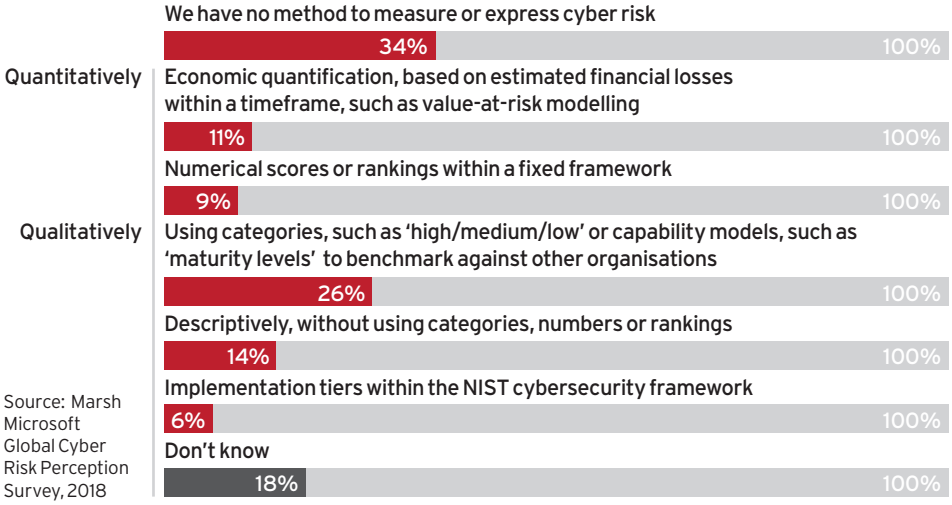
Corporate directors must embrace their oversight responsibilities for cyber risk management as they would for every other critical risk the organisation faces and should call upon key stakeholders, resources and organisational assets as needed to help them fulfil those duties. Cyber threats are a fact of life for every organisation today, but they need not be viewed as exotic, insurmountable challenges. By asking probing questions, tapping specialised expertise and positioning cyber risk as an enterprise issue requiring broad organisational accountability, directors can play a critical role in managing cyber risk with confidence.

This article is based in part on a webcast, 'Cyber Risk: A Corporate Directors' Briefing,' co-presented by the Marsh & McLennan Companies and WomenCorporateDirectors. Special thanks to Catherine Allen, Director, Synovus Financial Corporation, El Paso Electric Company and Analytics Pros; and Chairman and CEO, TSFG; and Kevin Richards, Global Head, Cyber Risk Consulting, Marsh, for insights provided on the webcast.

[1]https://www.jbs.cam.ac.uk/faculty-research/centres/risk/publications/space-and-technology/cyber-risk-outlook-2018/

FIG 6: MOST ORGANISATIONS THAT HAVE A MEANS TO EXPRESS THEIR CYBER RISK DO SO QUALITATIVELY

How does your organisation measure or express its cyber risk exposure?



Source: Marsh Microsoft Global Cyber Risk Perception Survey, 2018

FIG 7: INSURANCE OPTIONS AND COVERAGE CAN BE BASIC TO COMPLEX

INCREASING COMPLEXITY

COVERAGE SPECTRUM	RISKS
Basic cyber policy	■ Event management ■ Data privacy breaches ■ Network security liability ■ Privacy regulatory investigations ■ Cyber extortion ■ IT network business interruption ■ Restoration of data and cyber assets
Tailored cyber policy	■ System failure business interruption ■ OT system business interruption and security ■ IOT and product security risk ■ Network security regulatory investigations ■ Dependent network interruption
Property & casualty, cyber excess DIC or cyber gap exclusion buyback	■ 1st party property damage ■ Bodily injury/3rd party property damage ■ Intellectual property risks

Source: Marsh