BOARD OVERSIGHT OF CYBER RISKS AND CYBERSECURITY

DIDIER COSSIN

Professor of Governance and Finance
Founder and Director,
IMD Global Board Center

ABRAHAM LU

Research Fellow
IMD Global Board Center

Cybercrime – carried out using tactics such as stealing access credentials and infecting systems with malware, ransomware and phishing – poses a threat to data, processes, systems and customers.

MAY 2021

Even worse, cybercriminals might initiate a breach and exploit the incident by shorting the shares of their victims. Cybersecurity is therefore increasingly important for companies and individuals alike. The National Institute of Standards and Technology defines cybersecurity as "prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation."[1]

Cybersecurity and cyber risks have become a top issue in the boardroom. High-profile data breaches in recent years, including cyber risk events at Yahoo, Google, Facebook, Uber, Equifax and other companies, have led to many corporate crises. Cybersecurity and cyber risks have become a corporate governance issue for boards when they must hold CEOs accountable, face litigation or come under scrutiny from regulators.

The total volume of cyber events has increased dramatically year on year. More than 7,098 breaches were reported and 15 billion records were exposed in 2019 alone. The number of records exposed represents a 284% increase compared with 2018, according to a RiskBased Security report.[2] Cyber risks are growing fast, and this poses a material threat to the financial health of a company. It is imperative to understand the company's cyber damage in economic terms, given its enterprise-wide negative impact on strategy, finance, legal, compliance, operations and reputation. According to a report by Cybersecurity Ventures sponsored by Herjavec Group, cybercrime is projected to cost the world $6 trillion annually by 2021, up from $3 trillion in 2015.[3] In a survey conducted by Marsh and Microsoft, 28% of companies with revenue above US$1 billion reported that the worst potential loss value of a cyber incident could be over $100 million.[4]

Apart from the financial cost of cybercrime, a cyber incident can damage corporate reputation, brands and market value. In 2013, US retail giant Target experienced a data breach – credit and debit card details and the personal data of 70 million customers were stolen from the company's databases. The total damage was estimated to be over $18 billion. The company was criticized for being too slow to respond and report the breach to customers. Partly as a result of the breach, its sales dropped by 46% in the fourth quarter of 2013. The reputation of Target's board was tarnished when Institutional Shareholder Services (ISS) recommended against re-election of members of the board's audit and corporate responsibility committees for the "failure of the committees to ensure appropriate management of these risks ..."[5]

The widespread concerns about cyber risks and cybersecurity led to heightened attention from regulators. In response, the US Securities and Exchange Commission (SEC) offered companies some official guidance on cybersecurity disclosures in February 2018. The SEC makes clear that cybersecurity is not an IT issue. Rather, it is an integral component of a company's broader enterprise-wide risk management structure. Data breach notification laws have been enacted in the US since 2002. These laws "require individuals or entities affected by a data breach ... to notify their customers and other parties about the breach as well as [to] take specific steps to remedy the situation based on state legislature."[6] Breach notification legislation has significantly impacted businesses by defining whether, when, how and to whom notifications of a breach must be given. Regulators are tightening regulatory compliance, requiring effective cyber risk and cybersecurity governance structures at board level.

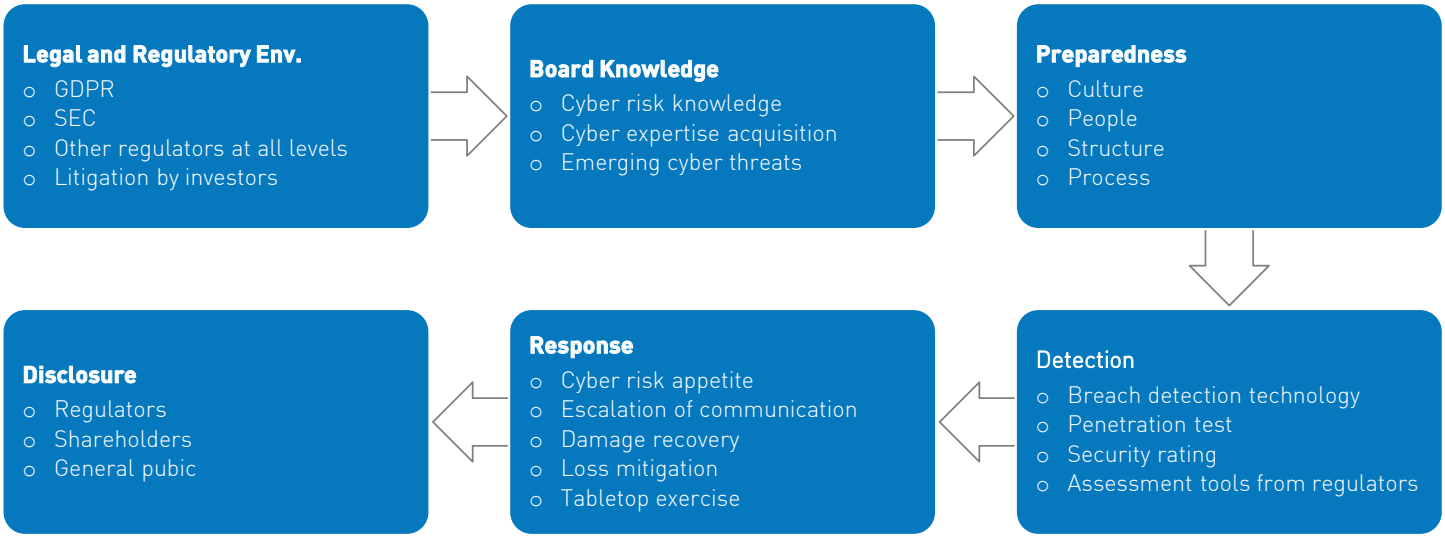
The board is charged with overseeing a company's cybersecurity risk. In response to the new challenges, the National Association of Corporate Directors (NACD) developed the Cyber-Risk Oversight Handbook, which proposes five often-cited principles:

1. "Directors need to understand and approach cybersecurity as a strategic, enterprise risk, not just an IT risk.
2. Directors should understand the legal implications of cyber risks as they relate to their company's specific circumstances.
3. Boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on board meeting agendas.
4. Directors should set the expectation that management will establish an enterprise-wide cyber-risk management framework with adequate staffing and budget.
5. Board-management discussions about cyber risk should include identification and quantification of financial exposure to cyber risks and which risks to accept, mitigate or transfer, such as through insurance, as well as specific plans associated with each approach."[7]

Cyber risk and cybersecurity are complex. This article aims to provide a framework to facilitate the task of boards and directors in carrying out cyber risk and cybersecurity oversight duties effectively. The active oversight role of boards requires them to understand emerging and constantly changing legal and regulatory environments. They also need to address any knowledge gaps to protect business

interests from current and future threats. Boards should be well prepared before a cyber breach occurs to avoid negative consequences resulting from inadequate oversight. Board oversight also means boards need to take an active role in detection and a response plan to ensure business continuity. Finally, board disclosure on cyber risk and cybersecurity should go beyond compliance. Indeed, boards should engage in meaningful dialogue with key stakeholders as all stakeholders, especially regulators, are paying close attention to cybersecurity risks. We propose six steps for boards to consider with respect to oversight of cybersecurity risks (see Figure 1).

Figure 1: Six steps for oversight of cybersecurity risks



The Legal and Regulatory Environment

Boards and directors need a clear picture of potential cyber threats, in order to evaluate and implement the appropriate response plan which is compliant with the law. First, they must understand the legal and regulatory implications related to cyber risks, cybersecurity and data protection. The legal and regulatory environment is evolving fast globally, so boards need to keep abreast of new legislation, law enforcement and regulatory agencies at different levels. Second, boards and directors are stewards of a company, so they need to ensure that adequate policies, oversight and responses are in place to meet the regulatory requirements. Failure to provide appropriate oversight might result in fines or damages levied by regulatory bodies. Third, apart from the potential liability facing their companies, boards and directors also face litigation from stakeholders, especially investors. Investors could target board members for a lack of oversight programs and capabilities.

The General Data Protection Regulation (GDPR)

Data breaches have prompted countries and regulatory agencies around the world to tighten data privacy laws. One of the toughest data privacy laws is the General Data Protection Regulation (GDPR), which came into force in the European Union (EU) in May 2018.

GDPR applies to companies operating in the EU that process personal data and imposes harsh penalties of up to 4% of global revenue for inadequate compliance.

GDPR expands individuals' control over the use of their personal data including access, rectification, erasure and restriction of processing. The objective of GDPR is threefold:

1. "This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.
2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.
3. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data."[8]

According to a UN study in 2020 on data protection and privacy legislation worldwide, 132 out of 194 countries had put in place laws and regulations to secure the protection of data and privacy. Out of the 194 countries, 66% had implemented legislation, 10% had draft legislation, 19% had no legislation and for 5% of counties, there was no data.[9] Wherever companies operate, the new data protection laws are pushing cyber risks and cybersecurity into boardroom. Boards need to understand how these laws and regulations apply to their businesses in all the jurisdictions they operate in. Directors must be aware of the regulations on the collection, use and sharing of personal information, and address any regulatory gaps.

The US Securities and Exchange Commission (SEC)

As a reflection of the growing number of cyber threats and incidents, the SEC has prioritized cyber risks and cybersecurity disclosure in recent years. The focus has shifted from generic disclosures to meaningful disclosures that help with investors' decision making, especially with regard to the legal and reputational risks resulting from cyber threats.

In February 2018, the SEC approved an "interpretive" release titled "Commission Statement and Guidance on Public Company Cybersecurity Disclosures," Release No. 33-10459 (Guidance).[10] This release updated and expanded the 2011 guidance on public company disclosure and other obligations concerning cyber risks and cybersecurity. The guidance highlights the importance of cybersecurity controls, policies and procedures, stresses timely notification of material cyber incidents, and reiterates insider trading prohibitions in the event of a significant cyber incident. The guidance also heightens focus on the role of boards in overseeing the management of cyber risk and cybersecurity.

Table 1 gives an example of a disclosure that was the subject of SEC comments. It includes the company's original disclosure, the SEC's comments and the company's amended disclosure. Cybersecurity and cyber risk disclosure should be detailed enough to enable the evaluation of cyber risks under the new disclosure requirement.

Table 1: Luckin Coffee Inc. and SEC

Luckin Coffee Inc. (Form DRS filing date 22 February 2019) **In Business section, User Privacy and Data Security, page 101:**	"Various laws and regulations, such as the Cyber Security Law of the PRC, govern the collection, use, retention, sharing, and security of the personal data we receive from and about our users. Privacy groups and government bodies have increasingly scrutinized the ways in which companies link personal identities and data associated with particular users with data collected through the internet, and we expect such scrutiny to continue to increase. We have adopted policies, procedures and guidelines to comply with these laws and regulations and protect the personal privacy of our customers and the security of their data."[11]
SEC comments (Form UPLOAD filing date 21 March 2019) **Numbered list – Number 10:**	"We note the disclosure here that you have adopted policies, procedures and guidelines to comply with cybersecurity laws and regulations and protect the personal privacy of your customers and the security of their data. We also note your risk factor disclosure on page 22 that you "have in the past and are likely again in the future to be subject to these types of attacks, although to date no such attack has resulted in any material damages or remediation costs." Since it appears that cybersecurity risks are material to your business, please disclose the nature of the board's role in overseeing your cybersecurity risk management, the manner in which the board administers this oversight function and any effect this has on the board's leadership structure."[12]
Luckin Coffee Inc. Amended disclosure (Form DRS/A filing date March 25, 2019): **In Business section, User Privacy and Data Security, page 110, the company added the following:**	"Our board of directors has general oversight power over cybersecurity issues and delegates the daily supervision responsibility to our chief executive officer, Ms. Qian. The head of our IT department directly reports cybersecurity status to Ms. Qian, and in case of a cybersecurity incident, Ms. Qian will report the incident to our board of directors to take appropriate and timely measures in response to the incident."[13]

The SEC has also brought cyber-related enforcement actions based on inadequate disclosures of cyber risks and cybersecurity. In September 2018, the SEC filed a case against Voya Financial Advisors. "The Commission filed settled administrative proceedings against an Iowa-based broker-dealer and investment adviser related to its failures in cybersecurity policies and procedures surrounding a cyber intrusion that compromised personal information of thousands of its customers, in violation of Reg S-P and Reg S-ID."[14]

US state governments, regulators and investigations at all levels

In the US, cyber risk and cybersecurity have become important issues for governments at all levels. On 11 May 2017, President Trump issued Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," to improve the country's cyber capabilities and modernize the government's information technology infrastructure. Congress, both the House of Representatives and the Senate, has also been focused on cyber risk and cybersecurity. Legislation has been introduced to address various issues, including mandating notification to consumers of data breaches, requiring a

comprehensive privacy and data protection program, and addressing the cybersecurity preparedness and responsiveness of public companies.

"In the US, both the Federal Trade Commission (FTC) and Consumer Financial Protection Bureau (CFPB) have brought data security enforcement actions. While relatively less active in the past year, the FTC has brought over 60 cases against companies alleging 'unfair or deceptive acts and practices' following data breaches. In March 2016, the CFPB brought its first data security enforcement action against a company for allegedly deceiving consumers about the company's data security practices and the safety of its online payment system." [15]

In the US, each state has data privacy and breach notification laws as state governments also pay attention to cybersecurity matters. For example, the California Consumer Privacy Act – considered one of the most expansive US privacy laws to date – took effect on 1 January 2020. Following a data breach, companies often face investigation by state attorneys. Equifax, after its massive data breach, faced inquiries from 50 state attorneys general. In 2017, the New York Department of Financial Services (NYDFS) imposed new cybersecurity requirements on financial services and insurance companies, dictating that boards must receive annual cybersecurity reports with detailed cyber resilience programs. Corporate directors should be aware that they might be personally accountable for failures in cyber risk oversight in different jurisdictions.

The nature of cyber threats varies by industry. Financial services, utilities and communications are industries that face more cyberattacks than others. Therefore, there are industry-specific laws with stringent cyber risk and cybersecurity requirements. We take the US as an example to introduce the complex legal and regulatory environment. However, boards should be aware that legal regimes vary from country to country, and firms must comply with the specific regulations in the countries in which they operate.

Litigation by investors

Companies may also face substantial civil litigation brought by various stakeholders in the aftermath of cybersecurity incidents. In general, directors could insulate themselves from lawsuits by showing that they have fulfilled their duty to act in good faith, with loyalty and due care, also known as the business judgment rule. Despite being protected by this rule, directors could still be liable for a failure of oversight. The Delaware Chancery Court, in its 1996 Caremark decision, declared that directors can be held personally liable for failing to "appropriately monitor and supervise the enterprise." Furthermore, litigation and regulatory enforcement actions have shown that cyber litigation has not been limited to lawsuits against companies. Following three data breaches between 2008 and 2010, Wyndham Worldwide Corporation's board was sued for negligence of fiduciary duty of care in the oversight of cyber risk and cybersecurity.

Regulators hold boards and directors to a high level of accountability by reminding them that cybersecurity is a high-priority issue that must be addressed from the top down. The board of directors has the ultimate responsibility for a company's cyber risk and cybersecurity. If boards fail to take this obligation seriously, they could be held accountable for any consequences. Directors could be ousted by institutional investors and activists and, to an extent, become targets of shareholder lawsuits.

In order to avoid potential litigation or regulatory actions, boards and directors should definitely step up their oversight and be proactive by establishing a comprehensive cybersecurity governance structure, hiring the right people, creating policies, formalizing processes, testing cybersecurity systems and crafting a data breach response plan. These are the key areas that the board and directors must focus on to fulfill their oversight obligations. To that end, directors should consider the following questions:

- Are you aware of data privacy legislation globally that might impact your business?
- How should the company deal with the diverse laws, regulations and rules that exist globally, nationally and locally? What is your compliance plan? Does your company monitor current and potential cybersecurity-related legislation and regulation actively?
- What is a responsible way to use, leverage and secure the data of your customers? How do you ensure regulatory compliance with GDPR, SEC and other laws and regulations? How do you prevent improper use of sensitive data?
- Does the board understand its role and responsibility in fighting cyberattacks?
- Are the board and directors aware of the negative impact (financial, legal and reputational) a cyber breach could have on them personally?

Board Knowledge of Cyber Risks and Cybersecurity

The role of the board and directors is to provide risk governance, a credible challenge to management and independent oversight. Directors should not micro-manage cybersecurity risks, but rather make sure that management is doing a good job by overseeing their practices. However, if directors lack understanding of the details of cyber issues, they might not understand all the ramifications of what executives tell them. To fulfill their oversight responsibilities, directors should address knowledge gaps proactively and the board should acquire profound cybersecurity expertise to protect corporate interests effectively.

Cyber risks knowledge

Cisco identifies seven common forms of cyberattack: Malware, phishing, man-in-the-middle attack (MItM), denial-of-service attack, SQL injection, zero-day exploit, and DNS tunneling.[16]

- Malware refers to several malicious software variants, for example worms, viruses, ransomware and spyware. Malware can be used to steal sensitive personal data or demand a ransom.
- Phishing is a type of cybercrime in which someone poses as a legitimate or reputable source and tries to steal sensitive data such as banking, credit card, login or personally identifiable information.

- MItM is also known as person-in-the-middle (PItM) or eavesdropping, whereby attackers secretly relay or intercept communications passing between two parties and make the victims believe they are communicating directly with each other. Attackers can inject fraudulent messages or steal information and identity.
- Denial-of-service attacks (DoS) happen when attackers flood corporate systems, servers or networks with huge volumes of traffic that trigger a systemic crash. The DoS attack makes networks inaccessible to legitimate users like employees or customers of banks, companies, governments and other institutions. Even if the attackers do not steal information, attacks are costly for the victim to handle.
- SQL (structured query language) injection occurs when an attacker interferes with the queries of an SQL database to retrieve information that would not normally be revealed. SQL injection can change data with malicious code and cause persistent damages to the server.
- A zero-day exploit happens when an attacker exploits a network or software vulnerability during a short window of time after the vulnerability is announced but before a solution is implemented. Zero-day attacks can adversely affect the performance of a network, software, data or computers.
- DNS (domain name system) tunneling occurs when an attacker uses the DNS protocol to extract data secretly or to send/receive data from a compromised server to an external malicious server.

Acquisition of cyber expertise

Without board-level cyber knowledge, directors could be frustrated by the challenges posed by cyber risk oversight responsibilities. Non-tech directors should attain a basic understanding of key cyber concepts. To develop the necessary expertise to challenge management and oversee complex cyber issues, directors need to follow some cyber literacy courses. The training should cover best cyber practices, cyber technologies and cybersecurity governance metrics. A cyber training program would provide advanced understanding of board directors' cyber oversight knowledge, demonstrating tangible qualifications to stakeholders their cyber capability.

Even with training, director-level cyber expertise could be weak. Given the size limit of a board, most boards have only one tech-savvy director. Adding more cyber-competent directors could improve the board's governance of complex cyber risk and cybersecurity issues. This would help the board get up to speed on cyber issues and understand their potential impact on overall corporate strategy. Asking questions will gather the right information to make decisions. Without cyber expertise, the board will find it difficult to make informed decisions.

As cyber technology moves quickly, directors might be concerned by the complexity of issues. Depending on the current board expertise and the complexity of cyber issues facing the company, the board may deem it necessary to leverage external advice. External expertise could help the board benchmark board cyber practices with peers and enhance its cyber competency.

Emerging cyber threats

In July 2020, members of the Cyber Risk Director Network met to explore emerging threats. The three emerging cyber risks that might affect longer-term company strategies are the spread of disinformation, attacks on information integrity and quantum technologies.[17]

The spread of disinformation, or "fake news," is spurred by the growth of social media, which allows cybercriminals, states, activists, unhappy employees or competitors to seek to gain advantage by spreading false information to deceive others. Artificial intelligence technology can be used to modify images, voices or videos to produce convincing deep fakes. The emerging attacks have become so sophisticated that the false rumor of a CEO's death in a car crash could cause the company's market capitalization to drop by billions of dollars. Deep fakes or disinformation can cause financial or reputational damages that are hard to reverse.

Attacks on information integrity occur when cyber criminals hack a computer system and modify data where it is being stored, making critical information "unreliable, unusable, or insidiously inaccurate in ways that have downstream impact."[18] Since it is difficult to detect or trace whether data has been corrupted, information integrity attacks can be more dangerous than data thefts.

Quantum technologies and quantum computers are less than 10 years away. The National Institute of Standards and Technology (NIST) suggests that by 2030, a quantum computer capable of breaking high security encryption could be built by large tech companies such as Google and IBM. Once they become commercially available, quantum computers will be able to break current public key encryption algorithms. Given the fast progress in quantum computing, quantum supremacy is going to transform industries in a disruptive way. Companies should deploy new types of encryption algorithms, since quantum computers will put all current systems, networks and servers at risk.

- With respect to boards' cyber risks and cybersecurity knowledge, directors should consider the following questions:
- What is the cost of global cybersecurity trends and cybercrime?
- Can you identify recent reported attacks and breaches – globally, in your country or your industry? What can you learn from these disaster stories?
- Are there cyber knowledge gaps in the boardroom?
- Has your board gone through a cyber risk and cybersecurity training program?
- What can current directors bring to the cyber risk and cybersecurity discussions now? How many new directors should the board recruit?
- Should the board leverage third-party expertise to benchmark with peers and validate the board's cyber readiness?
- What leading best board practices should you benchmark?

Board Oversight of Cyber Preparedness

When overseeing a company's cyber preparedness, board directors should apply the same common-sense approach that they apply to other business risks. A risk preparedness oversight approach should address issues related to culture, emphasizing that cybersecurity risk is not only an IT concern but also an enterprise-wide business issue. When establishing an oversight framework, the board should establish the right structure, hire the right people and address issues related to policies and processes to suit the type of company and its resources. This is to make sure that when cyber incidents happen, the company has the right team to respond with planned protocols to reduce any negative consequences. However, there is no one-size-fits-all solution. Any cyber preparedness framework implemented should be consistent with the overall risk management policies and corporate strategy.

Culture

As already noted, but worth repeating, cybersecurity risk is not a technology issue, it is business risk that affect the entire enterprise. Like all major risks, cyber risk and cybersecurity require a culture that drives individual awareness and commitment, since defensive tools will never be sufficient to prevent cyberattacks. In many cyberattacks, employees are often the major vulnerable points. Therefore, the whole organization should share responsibility, collaborate and undergo education and training if necessary, in order to contain and manage cyber risk. Each employee has a role to play in creating a culture of cybersecurity.

A cybersecurity culture starts with the "tone at the top" of both the board and senior executives. Boards are critical in setting the right tone, and senior management must walk the talk. Leading by the example is the only way to create a culture that promotes the right values and behaviors. Senior management must make cybersecurity a top priority, and boards need to make sure that senior management has a comprehensive plan – controls, tools, processes, systems, testing, training and protocols to follow in the event of a cyber breach. The right culture should reinforce the comprehensive plan, support its implementation and mitigate potential losses.

A strong culture of accountability should involve all employees, since they are often a weak spot if they are misinformed or inattentive. It is highly recommended to limit employees' access to sensitive information as a preventive measure. Top management needs to support thorough training across the organization to make employees understand that everyone has an obligation to protect the company from cyberattacks. Employees should be aware of typical cyberattack techniques and remain vigilant. It is also necessary to balance the conflicting interests between employees and the organization. Treating employees respectfully and fairly can reduce security risks from disgruntled and malicious employees.

People

At the senior management level, the CEO is accountable to the board for cyber risks and cybersecurity management. However, a CEO may look to the head of IT, the chief information officer (CIO) or the data protection officer (DPO) to

interact with the board and be accountable for cybersecurity risk management. Boards need to be aware that responsibility might be misaligned within the C-suite, which could leave companies vulnerable when it comes to combatting cybersecurity risk.

In the previous section, we discussed board cyber risk knowledge and expertise. One way the board could ensure that there is technological expertise in the management team is to establish the position of chief information security officer (CISO). A typical CISO has a deep background in cybersecurity technology, as well as in-depth experience in business and regulatory laws. Typical activities of the CISO role include ensuring an information security program is implemented effectively; implementing cybersecurity policies; allocating internal and external resources for the protection of systems and the overall cybersecurity budget; liaising between the C-suite, these with cybersecurity responsibilities and the board; ensuring regulatory and legal compliance; evaluating cybersecurity risks and measuring them against business priorities and tradeoffs.[19]

The CISO works between the business side and the IT or security side of the organization. He or she should be the executive responsible for the enterprise-wide operation of the cybersecurity risk program and advising the board on appropriate levels of response. The CISO should report to the CEO or the board, or its designated committee, on the state of cybersecurity and ensure adequate preparedness to prevent breaches, thus enabling the board's efficient and effective oversight.

The board of directors should make sure that even if the CISO reports directly to the CEO, he or she should have regular access to the board. Direct conversations help the board and the CISO to engage more deeply on cyber preparedness – insight into cybersecurity exposure, cybersecurity capabilities, the resources required, and benchmarking with industry leaders. This is also a signal that the board prioritizes cybersecurity risk preparedness and that all executives should support the cybersecurity infrastructure. Establishing a CISO position can enhance cyber resilience and promote business agility.

Structure

Board oversight of cybersecurity can be structured in many ways depending on the industry, company size, ownership, legal environment and current board risk management structures. Each company should choose the model most appropriate to its business. Whatever the structure, the board plays a crucial role in determining how the responsibility for cyber risks and cybersecurity should be shared across management, committees, functions and departments.

Who owns cybersecurity oversight at the board level? In general, the following entities could maintain the oversight responsibility:

- Full board
- Audit committee
- Risk committee
- Cybersecurity committee
- ...

In many companies, boards delegate cybersecurity oversight to the audit committee. The drawback is that the audit committee typically focuses on financial reporting rather than cyber risk assessment and response. Cybersecurity oversight requires technical expertise, which makes effective oversight challenging for the audit committee.

In other companies, boards rely on their risk committee to provide oversight of cyber risk management. The risk committee is responsible for overseeing enterprise-wide risk management policies and procedures. Since cyber risks are more consequential than other risks, it is crucial that the risk committee give cybersecurity a high priority.

A few larger companies have created a designated cybersecurity committee or a hybrid risk and cybersecurity committee to retain cyber oversight. The independent cybersecurity risk committee would focus exclusively on cybersecurity, data management and IT systems. Companies can decide whether to create an independent committee depending on the risk, data sensitivity, company size and business complexity. For example, GM created a Risk and Cybersecurity Committee to assist its board in fulfilling its oversight responsibilities with respect to the risk framework and "management's identification, assessment, and management of the company's key strategic, enterprise, and cybersecurity risks."[20]

Who is responsible for cybersecurity risk at the management level? A strong governance framework requires management to establish a centralized, cross-functional cyber risk management committee. The committee's core mandate is to ensure that the first line of defense is effective and efficient. It should prioritize cyber risks and cybersecurity strategy – protecting the company's crucial data and systems, detecting potential breaches and maintaining adequate response measures. The CISO could be the chair, with executives from key functions such as risk, operations, finance, compliance and public relations as members.

A cautious oversight structure would allow the board or designated board committee to meet regularly with the CISO or the cross-functional cyber risk management committee. Directors could also reach senior executives below the CISO to ensure that cyber risk defense measures are adequately implemented and bring awareness of emerging threats, such as disinformation, attacks on data integrity and quantum computation. As new threats continue to evolve, it is necessary for the full board to have a periodical concentrated review.

Process

Breaches in the past have shown that the board and directors are likely to face lawsuits as in the case of Wyndham's breach. Boards should play an important oversight role and be proactive in guiding management in the development of an effective process that should be followed by all employees.

A cyber program or cybersecurity risk process – put in place by the CISO or cyber risk committee – should detail the company's cyber risk appetite and tolerance, cybersecurity strategies, policies, procedures, systems, protocols, controls and budget. The well-documented, clear and concise plan should also address evolving regulations at all levels, provide accountability and track performance. The effectiveness of a cyber program depends on the quality of the input. Every

function – board, IT, legal, security, crisis management and data privacy – should be involved in developing the program. As a custodian of corporate information, the board itself handles sensitive and privileged corporate information. Therefore, boards should not be excluded from the company's cybersecurity risk process. Boards should also get involved in the implementation of the program, which we will discuss in the following sections.

It is a board's duty to understand and review the program periodically and evaluate its effectiveness to manage cyber risks over time. The board's evaluation should use appropriate benchmarks to regulatory requirements, industry standards and best practices. Like the board's oversight of other processes, such as audit, the evaluation process should provide the board with a clear overview of key cyber initiatives, the response plan and potential breaches.

The board might also consider hiring independent experts to review and report on the company's cyber program. The CISO or cyber risk committee might believe that the current cyber program is adequate for the company, but an independent expert can provide a candid assessment, which ensures that the program presented to the board is verified. External assessment can discover any blind spots or undetected vulnerabilities in the current processes and program. Boards work with independent cyber experts in the same way they work with auditing firms. In this way, the board can gain confidence in relation to key stakeholders such as regulators.

A key part of the oversight process is communication and reporting between the board and the CISO or cyber risk management committee. Reporting and communication should be transparent, timely, accurate and relevant, with both quantitative and qualitative content. Good reporting needs to be fit-for- purpose (non-technical) and allow the board to assess the cyber preparedness, identify gaps and benchmark improvement in an unbiased way. Effective communication will develop a trusting relationship between the board and the CISO, which will help the company respond quickly and effectively to cyber incidents.

The cyber-readiness framework outlined above, involving culture, people, structure and process, gives a sense of a company's cyber preparedness. It is critical for boards to have a mix of qualitive, quantitative and objective metrics to understand how effective the cyber program is. Through the board's leadership and oversight of preparedness, directors can fulfill their obligation to protect the interests of the company and all stakeholders. In terms of preparedness, directors should consider the following questions:

- How do you evaluate your company's culture related to cybersecurity? How does your company handle and oversee employees' privileged access to sensitive data? How do you train employees regarding privacy and security?
- Is your board comfortable with the company's cyber-risk management program?
- Does your board receive appropriate and meaningful cyber updates on a regular basis?
- How does your board rank in cyber preparedness compared with peers?

- What people, structure and processes do you have in place to ensure you are cyber ready? What are your company's cyber policies and procedures? When were they last reviewed by your board?
- Are you making adequate cybersecurity investments? What are the decision criteria for allocating the cyber-risk budget in terms of staff and money? Do you regularly evaluate the return on investment (ROI) on your cybersecurity controls?

Board Oversight of Breach and Vulnerability Detection

In addressing cybersecurity governance, companies should focus first on culture, people, structure and process. However, no matter what cyber program the company has in place, having the systems verified and assessed is a key step of the board's cyber oversight of breach and vulnerability detection.

Breach detection

The Mandiant Security Effectiveness Report 2020 found that 53% of attacks succeeded in infiltrating company systems without detection, and only 9% of attacks generated alerts.[21] Most intrusions were not detected by internal security processes, but rather by an external source such as law enforcement, external fraud monitoring or news reports.

Directors should be aware that detecting cyberattacks timeously has tangible effects on business. According to statista.com, the median time between cyber intrusion and detection was 11 days in 2019, significantly lower than the average 86 days in 2014.[22] There is a correlation between the days it takes to detect an intrusion and the cost of recovery. The Mandiant report found that organizations should aim to identify a breach within 100 days. The average cost of identifying a breach within this time was $5.99 million, rising to $8.70 million for breaches that took longer to identify.[23]

To detect breaches timeously and contain the damage, it is critical to have independent and external risk assessments proving that your security program is solid in detecting cyber incidents. The verification could be a penetration test or ethical hacking, a security benchmarking test or an assessment from regulators.

Penetration test

The board should consider a penetration test – also called pentesting or ethical hacking – to uncover weaknesses in the cyber defense system. A penetration test is a simulated cyberattack on a computer system, designed to search for vulnerabilities in a company's networks and applications. It is essentially a simulated hacker attack, whereby professional testers hired by the company use the same techniques as a criminal hacker and probe for weaknesses in a controlled form hacking.

A penetration test is performed to evaluate the security of the system and identify both weaknesses and strengths. It is designed to cause no real damage

and, if conducted when networks and systems are least used, the impact on daily operations can be minimized. Vulnerabilities could result from the system configuration, hardware or software flaws or operational blind spots. Through a full risk assessment, the company can immediately remediate any potential security weaknesses to detect breaches swiftly and enable critical data and systems recovery.

The board could designate internal testers to perform ethical hacking regularly. This is often preferable, since it is easier to contain the damage if breaches are detected sooner by internal staff. The company will also save money on external resources. When the company lacks adequate internal resources and expertise, the board should consider hiring first-class external expertise from independent cybersecurity firms or cybersecurity units at major accounting firms. However, since the tests could leave sensitive data exposed to external venders, the board should be aware of the risk and exercise proper oversight and control of the contracts.

Security rating

After a penetration test, the board could consider obtaining a security rating or cybersecurity rating to improve breach detection. According to Wikipedia, "Security ratings are an objective, data-driven, quantifiable measurement of an organization's overall cybersecurity performance. Security ratings provide businesses and government agencies with a third-party, independent view into the security behaviors and practices of their own organization as well as that of their business partners. Security ratings are a useful tool in evaluating cyber risk and facilitating collaborative, risk-based conversations."

A security rating assigns a security score to a company's cybersecurity performance. It works in a similar way to credit ratings, whereby rating agencies assign a credit score that measures a company's creditworthiness. Cybersecurity rating could become an important factor when evaluating the risk of any business relationship. Adoption of these services is on the rise and security rating could become as important as credit rating.

The board can look at the company's security rating and benchmark the effectiveness of its cyber program with best practices. Directors can look at common cyber incidents in the industry, time to detect a cyber incident, time to mitigate breach impact, time to restore critical systems, and time to recover sensitive data. These factors can all be benchmarked against peers, which will help give the board a real sense of cyber breach and vulnerability detection, as well as making mitigation of the negative impacts easier.

Assessment tools from regulators

Recognizing the increasing sophistication and volume of cyberattacks, many regulators have collaborated with industry to develop a cyber-risk assessment framework. These standards, guidelines and practices are designed to manage and reduce cyber risks. For example, in the US, the Federal Financial Institutions Examination Council (FFIEC) developed the Cybersecurity Assessment Tool to help institutions identify their risks and determine their cybersecurity preparedness.[24] The assessment tool enables financial institutions to discover any cyber breach in a timely manner and to limit the damage through continuous security monitoring and breach detection.

In August 2019, FFIEC issued a press release emphasizing the benefits of using a standardized approach to assess and improve cybersecurity preparedness. The members note that firms adopting a standardized approach are better able to track their progress over time, and share information and best practices with other financial institutions and with regulators.[25] There are a variety of standardized frameworks, including the FFIEC Cybersecurity Assessment Tool, the National Institute of Standards and Technology Cybersecurity Framework, [26] the Financial Services Sector Coordinating Council Cybersecurity Profile and the Center for Internet Security Critical Security Controls.[28]

Although these standardized tools are designed to support institutions in their self-assessment activities, they also help institutions understand regulators' expectations. For example, many regulators, including the Federal Reserve, the Office of the Comptroller of the Currency, The National Credit Union Administration and the Federal Deposit Insurance Corporation, implement FFIEC's Cybersecurity Assessment Tool as part of the examination process when benchmarking and assessing institutions' cybersecurity preparedness. FFIEC's Cybersecurity Assessment Tool classifies cybersecurity maturity into five levels – baseline, evolving, intermediate, advanced and innovative. This allows boards and directors to assess their state of governance in terms of the oversight of cybersecurity readiness. For details, see FFIEC's cybersecurity maturity classification system.

Through the board's oversight of breach and vulnerability detection, the company can send a clear signal that the board and directors are attentive to cyber risk and cybersecurity management. To assess the company's cyber breach and vulnerability detection capability, directors could consider the following questions:

- How is your board's oversight ranked in terms of cybersecurity maturity using the FFIEC tool?
- How vulnerable is your industry? At what point would your company know that it was under attack?
- How did your company perform in the last penetration test/ethical attack? How many times per year does your board authorize these tests? If none, why?
- How does management allocate outsourced resources? Are adequate resources devoted to breach and vulnerability detection?
- Do you hire external vendors to implement cybersecurity rating and regulator assessment tools? How does your cybersecurity score compare with that of peers and the industry average?
- Is your board aware of the risk of hiring external vendors? Do you have proper policies in place to control third-party risks?

Board Oversight of Cyber Response

It is not the board's responsibility to micromanage cybersecurity. However, in the event of a material cyber incident, it should engage in a deep dive. These are times when the board needs to get involved in the tactics and implementation of a response strategy. Board involvement will allow the company to respond appropriately and quickly, as the event could lead to reputational and regulatory backlash.

The possibility of a cyber event should be considered as a "when" not an "if," since nobody can guarantee that a company's cybersecurity program will not be breached. In this regard, it might be necessary to have a crisis response team including internal representatives such as IT, legal and management, with possible input from external advisors such as public relations, forensic and law firms. Individual member of the crisis response team should have clear roles and responsibilities.

A fundamental component of any cybersecurity program is response and recovery, which requires board oversight. The board needs to ensure a response plan is in place to define risk appetite in association with damage estimation, escalate communication when necessary, recover critical data and systems, and mitigate losses to enhance resilience. The response and recovery plan should be tested and refined through a tabletop exercise, so that no key steps of the incident response are missed.

Cyber risk appetite

An effective incident response plan starts with gathering incident information. This is to determine which systems have been breached and any potential damage; both should be checked against the predefined cyber risk appetite. The board and management are generally responsible for setting the cyber risk appetite as part of the company's cyber risk program.

Cyber risk appetite is the level of cyber risk that an organization is prepared to tolerate. An RSA article proposes that a good first step toward determining appetite is identifying and classifying applications, databases, systems, and information based on importance. The most important are mission- and business-critical systems, followed by the core infrastructure and extended ecosystem; last are the external, public-facing systems and points of interaction.[30]

Focusing on the mission- and business-critical systems is to ensure business continuity. The board must prioritize according to what would cause the most damage and have a response plan prepared.

Additionally, the company could have standard procedures for measuring potential damage resulting from cyber risk. Quantification is a more precise way to set the appetite. However, quantifying cyber risk damage is not always possible, since this would involve calculating both intangible and tangible aspects, depending largely on the nature of the business, objectives, regulations and legal exposure. In this case, risk appetite can be defined by broad loss levels or in a qualitative way.

Quantifying cyber risk helps the board make informed decisions about cyber risk appetite, which will help the company know where to allocate resources. The company can take on cyber risk below a certain level of loss, but beyond that level, management must escalate communication.

A precise estimate of the financial cost of damage resulting from cyber risk determines insurance coverage, and successful mitigation of losses also reduces pressure from stakeholders.

Escalation of communication

Board oversight ensures that an escalation process is in place to determine who should be notified internally and when. The board should be fully informed when a cyber incident occurs, especially when potential losses exceed a certain threshold. The board should work with management to decide who should be notified of an incident first. In general, the CISO would be the first to know and would then follow the predefined cyber risk appetite and report up the corporate ladder to the CEO, the risk committee and, ultimately, the full board. In some cases, external parties such as cybersecurity insurers should also be informed timeously. The escalation procedure should be periodically assessed.

Damage recovery

In a serious cyber breach, the board should oversee management in implementing a robust disaster recovery plan to minimize the damage and resume normal operations quickly and smoothly with the least disruption of activities. The cyber incident response plan should have concrete procedures established to deal with all potential threats (e.g., malware, phishing, man-in-the-middle attack, denial-of-service attack, SQL injection, zero-day exploit, DNS tunneling). Restoration activities could involve external parties such as the website hosting provider. Thus, the company should keep multiple means of communication with key contacts of suppliers. When the time comes for restoration and remediation, all internal and external personnel would be contacted immediately and mobilized efficiently.

Loss mitigation

Although damage recovery after a cyberattack enables a company to minimize losses and resume normal operations, it does not eliminate risk, so the company may need to purchase insurance to mitigate any further losses. Regular insurance is usually not sufficient; cybersecurity insurance covers any damage associated with cyber risk, including managing the fallout from the event, such as notification costs; business interruption; cyber extortion, such as the cost of investigation and reimbursement; and network security and privacy, such as payment of settlements and damages.[31]

Board oversight ensures that the company has the relevant cyber insurance. The board should ensure that management is familiar with the protocol for purchasing the cyber insurance, what cybersecurity insurance is required, whether the insurance cover is adequate, who would lead forensic investigations, and how quickly any incident should be reported to insurers. Directors might also take this opportunity to review their own liability insurance policies in the event of a cyber breach.

Tabletop exercise

No matter how good a cyber response plan is, it is always better if it has been tested and fine-tuned. Board oversight ensures that the response plan undergoes regular stress testing. In high-impact scenarios, board and management need to make critical decisions urgently, which could lead to mistakes that aggravate an already chaotic situation. A tabletop exercise, mock breach exercise, stress testing or simulated crisis could help directors and management clarify roles, remedy defective procedures, reinforce capabilities, prepare staff for action, and instill confidence in a controlled environment. Such exercises could make a real cyber crisis less stressful and damaging.

According to the Cyber Management Alliance, "In its simplest description, a Tabletop Exercise is a verbally-simulated scenario which can have a serious business impact if it were to occur in real life. During the exercise, attendees are encouraged to actually respond to the scenario as they would do if it were real. They then review their actions and discuss how things could have been handled better. These scenarios are organization-specific and are highly interactive, enabling tangible cross-departmental collaboration and communication."[32] For more details, see the Cyber Management Alliance article.[33]

At a basic level, a tabletop exercise can involve just key personnel such as IT specialists. At a more elevated level, board, senior management, public relations, compliance and legal counsel might participate periodically. At the highest level, a tabletop exercise might involve a broader crisis response team including board, senior management, employees around the world, together with external parties such as crisis managers, law firms and forensics consultants. The exercise would follow a simulated procedure to make the necessary notifications to customers, insurers, law enforcement and regulators, which should happen automatically if a crisis occurs.

As we have seen, the board should oversee a cyber response plan focusing on cyber risk appetite, escalation of communication, damage recovery, loss mitigation and a tabletop exercise. With these disciplined and regular preparations, the board would identify any vulnerabilities in the response plan, address any issues and suggest the necessary changes. Board oversight would help a company to respond to a cyber crisis effectively and efficiently. In the same way, directors can mitigate the risk of potential lawsuits or other liabilities from stakeholders.

To assess the company's cyber response capability in the face of a cyber crisis, directors could consider the following important and relevant questions:

- What is the company's cyber risk appetite? What losses would be catastrophic?
- What are your mission- and business-critical systems? How long can you survive without these systems?
- How often does your company experience a cyber incident? What is the protocol for elevating a cyber breach incident to the board? What is the threshold, e.g. financial impact of a cyber incident, for notifying the board?

- How fast will the company resume normal activities following a specific type of cyber-attack? Who makes critical decisions, such as paying ransom to recover critical business files? How should you keep critical business files safe –sufficient backups or encrypted data?
- What cyber insurance does the company have? Is the cover sufficient? How did you determine the cover?
- How comprehensive is the cyber crisis response plan? How often is it tested via a tabletop exercise? At which level should the tabletop exercise be conducted?
- What can you learn from other companies that mishandled a cyber crisis after a publicly disclosed breach?

Board Oversight of Cyber Disclosure

Much of board oversight focuses on cybersecurity preparedness, detection and response, as discussed above. However, the rules and regulations are changing around disclosure to the public in terms of cybersecurity. The EU's GDPR requires companies operating in Europe to disclose data breaches to national authorities within 72 hours or face heavy fines. As part of the post-breach management, each company should have plans in place for disclosure controls and procedures.

In most cases, it is not the board's responsibility to speak publicly about the breach. However, the board should oversee a disclosure plan before a breach occurs and disclosure implementation in the aftermath of a cyber breach, as this often drives relationships with regulators, shareholders and the public.

Regulators

For public companies, regulatory non-compliance is often associated with a legal penalty if there is a material breach. In the US, each state sets the level of the fine. In Arizona, for example, the maximum fine per breach is $500,000. The board should ensure that the company can demonstrate to regulators good faith efforts to prevent cyber risks and disclose any material breach. If directors can make a case that the company has followed the industry standards and best practices, penalties due to cyber incidents may be reduced.

Directors should also be aware of notification costs imposed by local governments. For example, Alabama can impose a fine of $5,000 per day for failure to comply with its notification law. Compliance failure could lead to more legal, financial and reputational costs. The board should oversee the disclosure procedure, so that the company does not fail to comply with the notification law amid the chaos.

In the US, the SEC issued interpretive guidance on cybersecurity disclosures, including restrictions on trading by insiders if the company is investigating a cyber breach. There is a risk of corporate insiders trading in advance of a company's public disclosures regarding a material cybersecurity breach. The board should be mindful of potential law enforcement actions against the company and individual executives for insider trading. It goes without saying that enforcement actions would have a significant reputational impact on the company.

Investors

The board should also be aware that institutional investors are increasingly focusing on risk governance and cybersecurity. Once they find that board oversight of cyber risk has been lacking, they can target the company with lawsuits. To fend off investor lawsuits, the board needs to demonstrate that there is adequate expertise among the directors, with proper cyber and legal background training. The board should also be ready to answer questions from institutional investors. If the board works proactively with management to oversee the development of a comprehensive cybersecurity program, investors will know that the company has taken the cybersecurity and cyber risks seriously.

The board could develop its own cybersecurity oversight manual covering the legal and regulatory environment; cyber knowledge on the board; preparedness (culture, people, structure and process); detection (breach detection, penetration test, security rating and assessment tools from regulators); response (cyber risk appetite, escalation of communication, damage recovery, loss mitigation and tabletop exercise); and disclosure (regulators, investors and general public). A fully prepared board will dramatically reduce the risk that investors take action against the company.

General public

Advised by the legal department and public relations, the board and management need to work together on a disclosure plan to define which leaders will speak publicly and what information should be disclosed. The plan should be flexible enough to adapt to the evolving scope of the incident. There have been cases in which the CEO who was supposed to speak to the public was ousted and the chairman of the board had to step up, as happened at BP in the wake of the Deepwater Horizon oil spill in the Gulf of Mexico in 2010. Although directors should not talk to the press, being prepared to face the media in case of an emergency is important for the board to control the narrative and reduce public concern about a cyber breach.

In sum, the board needs to scrutinize the different expectations and requirements of stakeholders before a cyber incident occurs and craft a disclosure plan to address various scenarios. In the aftermath of a cyber incident, the board needs to oversee the appropriate implementation of the plan. Directors could consider the following questions:

- Who is authorized to communicate to key stakeholders in the event of a major cyber crisis? How prepared are lower-level customer-facing employees in the event a breach, e.g., call center staff?
- What are the company's procedures for reporting the cyber incident to the authorities such as law enforcement and regulators?
- How and when should the company communicate with all other stakeholders? Should the company disclose to the press, employees, suppliers, investors and customers at different times?
- What is the company's plan to stop insider trading when the company is investigating a cyber breach?
- How effective are the company's disclosure processes when benchmarked against the industry leaders and the best practices?

Conclusion

Cyber risk has escalated so rapidly that organizations worldwide are scrambling to keep up with the evolving cyber threat. Cybersecurity has become a business issue and one of the pillars of strong companies. To ensure protection from cyber risks, companies should involve every level of the organization. Management should be accountable for maintaining strong cyber preparedness, detection, response and disclosure processes. The board should make cybersecurity a top priority and develop its governance framework – not sitting back but leaning in – to add the right insights and ask the right questions. Effective and efficient cybersecurity governance is key to prevent negative consequences resulting from a cyber breach, to ensure regulatory compliance and to satisfy the board's duty of care.

- For the board of directors, it is critical to understand the legal and regulatory environment such as GDPR, SEC disclosure standards, and laws and regulations facing international companies.
- If the board lacks expertise on the subject, it is advisable to add expert directors and let the full board go through cyber training on existing and emerging cyber threats. Adequate time to discuss cybersecurity issues should be allocated on the board agenda.
- The board needs time on its agenda to oversee cyber preparedness – setting the tone at the top with the right culture, choosing capable people to be accountable for the risk, establishing an efficient corporate structure, and developing the process.
- The board should also look for weaknesses and vulnerabilities – asking questions about breach detection technology, penetration tests, security rating and assessment tools from regulators. It needs to have sufficient information about IT systems, which are appropriately assessed and benchmarked by a third party.
- As an integral part of the oversight, the board needs to focus on its cyber incident response – determining the company's cyber risk appetite, setting the threshold for escalation of communication, limiting damage resulting from a data breach and implementing a recovery plan, mitigating further losses with cybersecurity insurance, and participating in and overseeing a tabletop exercise.
- For the board of directors, it is necessary to oversee cyber risk disclosure procedure, focusing mainly on understanding and anticipating the disclosure requirements from regulators, investors and the public.

In general, directors are protected by the business judgment rule, which assumes that they have exercised due care for the company and acted in good faith, unless it can be proved otherwise. However, if the plaintiffs have proof that directors have breached their fiduciary duties, directors can still be personally liable for a failure of oversight.

This is particularly true when there is a complete and systematic failure at overseeing and implementing the cyber risk and cybersecurity program in the company. By allocating adequate board time, looking for vulnerable areas and asking targeted questions, the board gives cyber risk and cybersecurity oversight priority and shows stakeholders that the company has adopted effective defenses.

Cybersecurity is a complex and dynamic issue. The best practices and standards may vary by country, region, industry and company, which means that the right approaches should be adapted accordingly to different laws, regulations and practices. Since the possibility of a cyber incident is not an "if" but a "when," the board ought to stay vigilant and actively engage in preparation, detection, response and disclosure. Even though the risks cannot be eliminated entirely, proactive and active oversight will lower the probability of a serious cyber incident occurring and reduce the losses, which can potentially be fully mitigated by cybersecurity insurance cover.

CYBERSECURITY EXERCISE

Your company is a JV between Company A and Company B. It has a large foreign cap and has been publicly listed since 2017.

Company A has two members on the board. The rest of the board, including yourself, are from Company B, as are most of the staff.

You have been informed, along with the other board members, that various company systems have been infected by several types of malware (e.g. viruses, worms, ransomware). There are no signs of the core systems having been attacked at the time.

Most of the malware consisted of zero-day exploits, i.e., previously undetected computer or software weaknesses. Until now, the company has largely relied on a classic antivirus software that can only detect known threats.

The CEO had a feeling that her emails were being read by those who were not the recipients, both internally and externally. There was also concern that the company had failed with four previous bids for business, in each case by a slim margin and always against the same competitor. It seemed that costs were being elevated to the exact affordable point of the company each time.

The CEO asked the COO to make inquiries.

Further analysis revealed that the core systems were being systematically attacked and a remote access tool (RAT) had been deployed, allowing an attacker to remotely control computing resources as if he was part of the company's staff.

The attack seemed to have the profile of an APT (advanced persistent threat). The hackers may have wanted to access private information on costs, prices, bids and intellectual property, including technology and innovations. Although elements of the intelligence process seemed pretty basic (e-mails forwarded to unknown addresses), others were more sophisticated, and it is unclear how much of the whole operation has been uncovered so far.

Recent media reports note that the US National Security Agency (NSA) and the United Kingdom National Cyber Security Centre (NCSC) have released a joint advisory on advanced persistent threat (APT) group Turla — widely reported to be Russian and also known as Snake, Uroburos, VENEMOUS BEAR or Waterbug. Turla uses the malicious Neuron, Nautilus and Snake tools to steal sensitive data and hide behind various foreign states' infrastructure and resources. The attacks thus at first appear to be made by foreign states but they seemingly also serve commercial purposes.

IMD Professor Didier Cossin and Elisabeth Bourqui prepared this exercise as a basis for class discussion rather than to illustrate either effective or ineffective handling of a business situation.

Sources

[1] NIST, Computer Security Resource Center. 2020. https://csrc.nist.gov/glossary/term/cybersecurity. Retrieved on 21 December 2020.

[2] RiskBased Security. 2020. 2019 Year End Report. https://pages.riskbasedsecurity.com/hubfs/Reports/2019/2019%20Year%20End%20Data%20Breach%20QuickView%20Report.pdf. Retrieved on 5 March 2021.

[3] Cybersecurity Ventures. 2020. The 2020 Official Annual Cybercrime Report. https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report/. Retrieved on 20 August 2020.

[4] Marsh and Microsoft. 2018. By the Numbers: Global Cyber Risk Perception Survey. https://www.marsh.com/us/insights/research/global-cyber-risk-perception-survey.html. Retrieved on 5 October 2020.

[5] Tapestry Networks. 2015. Cyberrisks and cybersecurity. https://www.tapestrynetworks.com/sites/default/files/publication_pdf/EACLN%20ViewPoint%20-%20Cybersecurity%20-%208-9%20April%202015%20SCORES.pdf. Retrieved on 21 August 2020.

[6] Wikipedia. 2020. Security breach notification laws. https://en.wikipedia.org/wiki/Security_breach_notification_laws. Retrieved on 21 December 2020.

[7] NACD and ISA. 2020. Cyber-Risk Oversight 2020. https://isalliance.org/isa-publications/cyber-risk-oversight-handbook/. Retrieved on 10 September 2020.

[8] The General Data Protection Regulation (GDPR), https://gdpr-info.eu/art-1-gdpr/. Retrieved on 24 August 2020.

[9] UNCTAD.org, https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx. Retrieved on 24 August 2020.

[10] The SEC. 2019. Commission Statement and Guidance on Public Company Cybersecurity Disclosures. [Release Nos. 33-10459; 34-82746]. https://www.sec.gov/rules/interp/2018/33-10459.pdf. Retrieved on 24 August 2020.

[11] SEC. Luckin Coffee Filing. 2019. https://www.sec.gov/Archives/edgar/data/1767582/000091205719000058/filename1.htm. Retrieved on 21 December 2020.

[12] SEC. Luckin Coffee Filing. 2019. https://www.sec.gov/Archives/edgar/data/1767582/000000000019005368/0000000000-19-005368-index.htm. Retrieved on 21 December 2020.

[13] SEC. Luckin Coffee Filing. 2019. https://www.sec.gov/Archives/edgar/data/1767582/000091205719000118/filename1.htm. Retrieved on 21 December 2020.

[14] SEC. 2020. Cyber Enforcement Actions. https://www.sec.gov/spotlight/cybersecurity-enforcement-actions. Retrieved on 24 August 2020.

[15] Francis J Aquila and Nicole Friedlander. 2018. Board oversight of cyber security. https://www.financierworldwide.com/board-oversight-of-cyber-security#.X0O39sj7RPY. Retrieved on 24 August 2020.

[16] Cisco. What Are the Most Common Cyber Attacks? https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html. Retrieved on 27

August 2020.

[17] Cyber Risk Director Network. 2020. Emerging Cyber Risks. https://www.tapestrynetworks.com/publications/emerging-cyber-risks. Retrieved on 10 September 2020.

[18] Ibid.

[19] Cisco. Chief Information Security Officer/Chief Security Officer. https://learningnetwork.cisco.com/s/article/chief-information-security-officer-chief-security-officer. Retrieved on 14 January 2021.

[20] GM Risk and Cybersecurity Committee Charter. 2019. https://investor.gm.com/static-files/4cac4315-7559-421c-84df-8ddff9cadf1d. Retrieved on 10 September 2020.

[21] Mandiant Security Effectiveness Report. 2020. https://www.fireeye.com/current-threats/annual-threat-report/security-effectiveness-report.html. Retrieved on 16 September 2020.

[22] Statista.com. 2020. Median time period between intrusion, detection, and containment of industrial cyber attacks worldwide from 2014 to 2019. https://www.statista.com/statistics/221406/time-between-initial-compromise-and-discovery-of-larger-organizations/. Retrieved on 16 September 2020.

[23] ITgovernance. 2019. How long does it take to detect a cyber attack? https://www.itgovernanceusa.com/blog/how-long-does-it-take-to-detect-a-cyber-attack. Retrieved on 16 September 2020.

[24] The Federal Financial Institutions Examination Council (FFIEC). 2017. The Cybersecurity Assessment Tool. https://www.ffiec.gov/cyberassessmenttool.htm. Retrieved on 16 September 2020.

[25] FFIEC. 2019. FFIEC Encourages Standardized Approach to Assessing Cybersecurity Preparedness. https://www.ffiec.gov/press/pr082819.htm. Retrieved on 18 September 2020.

[26] NIST. Cybersecurity Framework. https://www.nist.gov/cyberframework. Retrieved on 18 September 2020.

[27] FSSCC. Financial Services Sector Cybersecurity Profile. https://fsscc.org/Financial-Sector-Cybersecurity-Profile. Retrieved on 18 September 2020.

[28] Center for Internet Security. CIS Contorls. https://www.cisecurity.org/controls/. Retrieved on 18 September 2020.

[29] FFIEC. 2017. Cybersecurity Maturity. https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_May_2017_Cybersecurity_Maturity_June2.pdf. Retrieved on 18 September 2020.

[30] RSA. 2016. Cyber Risk Appetite: Defining and Understanding Risk in the Modern Enterprise. https://www.rsa.com/content/dam/en/white-paper/cyber-risk-appetite.pdf. Retrieved on 22 September 2020.

[31] Holly J. Gregory, Sidley Austin LLP. 2020. Board Oversight of Cybersecurity Risks. https://uk.practicallaw.thomsonreuters.com/5-558-2825?__lrTS=20200813052351205&transitionType=Default&contextData=(sc.Default)&firstPage=true. Retrieved on 22 September 2020.

[32] Cyber Management Alliance. 2020. Cybersecurity tabletop exercises and why you can't ignore them in 2020. https://www.cm-alliance.com/cybersecurity-blog/cyber-security-tabletop-exercise. Retrieved on 25 September 2020.

[33] Cyber Management Alliance. 2020. Cybersecurity tabletop exercises and why you can't ignore them in 2020. https://www.cm-alliance.com/cybersecurity-blog/cyber-security-tabletop-exercise. Retrieved on 25 September 2020.

Contact us

Quentin Dufresne
IMD Global Board Center
Tel: +41 21 618 02 65
www.imd.org/boardcenter
boardcenter@imd.org

The IMD Global Board Center

The IMD Global Board Center is committed to supporting your company's long-term success through its board performance. Our unique combination of open and customized board education programs aims to develop your board's competitive advantage and realize its full potential. These programs bring together world-class thought leadership, our own cutting-edge governance research and inspiration from best board practices of leading organizations in Asia, Europe, the Americas and the Middle East.

Chemin de Bellerive 23
P.O. Box 915
1001 Lausanne
Switzerland
Central tel: +41 21 618 01 11
Central fax: +41 21 618 07 07
info@imd.org
www.imd.org