Cyber Loss Mitigation For Directors

Cyber Loss Mitigation For Directors

Prepared by Dan A. Bailey, Bailey Cavalieri LLC
for Chubb

Note: The views, information and content expressed herein are those of the author and do not necessarily represent the views of Chubb.

Contents

Introduction

Cyber risk has become a major potential loss exposure for almost any company. Although nonexistent just a few decades ago, cyber risk today can cause devastating harm to a company and its employees, customers, vendors, constituents and reputation. Not surprisingly, as businesses have become more reliant on technology, the resulting risks have become far more complex and potentially harmful.

Cyber exposures come from a wide variety of sources, including terrorists, hackers, criminals, competitors, and employees, as well as simple mistakes and inadvertent misuse or loss of data. Even the most vigilant company can be a victim of a cyber incident, data breach or another cyber loss. Class-action lawsuits, huge forensic and mitigation costs, notification and credit-monitoring services, and data restoration efforts can result in tens or even hundreds of millions of dollars of loss to a company. State attorneys general, federal and state regulators, and plaintiffs' lawyers are all likely and formidable adversaries for a company if something goes wrong. In addition, the company's computer systems may be shut down, critical data may be lost or stolen, and business operations may be interrupted for an extended period. Often the most severe consequence, however, is harm to the company's reputation, which can take years to restore.

As with any other exposure, directors should confirm that reasonable steps are taken to identify, mitigate, respond to, and recover from third parties relating to cyber-related problems when they arise. However, because of the potentially severe nature of this risk, the directors' oversight role in this area should be particularly robust and is far from easy. This booklet identifies a number of specific practices and strategies that directors can follow to manage cyber risk. However, in light of the rapidly evolving nature of technology and the unique aspects of cyber risk for different companies, no booklet can describe procedures or policies that fit all companies and no company should be expected to adopt all the practices discussed.

Two distinct timeframes should be considered when identifying directors' loss mitigation practices in this context.

- First, what should directors do prior to a cyber incident to manage the risk and mitigate potential consequences? No company can prevent all cyber attacks, but directors can implement and oversee various initiatives that can reduce the likelihood of a cyber incident and the harm it may cause.
- Second, when a cyber incident occurs, how should directors respond and is the company prepared to recover? How a company, including its directors, reacts to a cyber incident in the hours, days, and weeks following discovery of the incident is at least as important as risk management activities prior to the incident.

This booklet addresses loss prevention ideas for each time frame and the legal duties of directors.

Types of Organizations Impacted

A common myth is that only large, for-profit companies with lots of customer data should be concerned about cyber risk. In reality, almost any organization–for-profit, nonprofit, large, small–can be a victim of a cyber incident.

Nonprofit entities are in some respects even more vulnerable to cyber attacks than are large, for-profit companies because nonprofits' systems are likely to be less sophisticated or lacking all of the latest tools. Hackers may try to obtain client and donor data (including credit card information), employee records, confidential communications, and financial information from nonprofit entities' electronic files. Nonprofit organizations performing sensitive work on political, religious, ethical, or cultural issues can be especially high-risk targets. Plus, nonprofit entities can attract a wider array of threat actors. In addition to thieves and other self-interested criminals, activists who disagree with missions or operations of organizations can be greater threats to nonprofit entities than to for-profit companies.

The cyber loss mitigation strategies discussed here can apply to both for-profit and nonprofit organizations. The main differences in strategies relate to scale and available resources. Nonprofit entities can implement other simple concepts to supplement the strategies described here. For example, limit the amount of client and donor information collected to only the bare essentials. Too many nonprofits collect much more information than needed because it is easy to do so, thereby increasing the harm an attack can cause.

Directors’ Cyber-Related Legal Duties

For the most part, losses incurred by directors arising out of cyber attacks have not been significant to date, even for large and highly publicized cyber incidents. Injured third parties generally do not have standing to sue directors. Claims of director mismanagement face formidable defenses under the business judgment rule and state exculpatory statutes, and securities class-action lawsuits have (so far) been rare because a company’s stock price typically has not suffered a large and/or immediate drop in market value following the announcement of a cyber incident.

However, that favorable loss environment for directors may not continue. As cyber incidents continue to increase in number and severity, shareholders, regulators, and courts (among others) will likely subject director behavior to ever-increasing scrutiny, criticism, and accountability. Existing legal standards can support that heightened director exposure as summarized later on. However, when combined with the inevitable new laws, regulations, and guidelines that will likely be adopted as cyber concerns increase, the legal environment for directors in its context will only worsen. Directors who fail to understand and properly discharge these duties not only expose themselves to legal consequences but also increase the likelihood of potentially catastrophic harm to their companies and constituents.

The following summarizes several of the more important regulations involving cyber risk that are currently applicable to directors.

Fiduciary Duty
A basic fiduciary duty for any director is the duty of care. As consistently recognized by state statutes and court decisions for decades, a director is required to act as a reasonably prudent person would act under similar circumstances. This is a fluctuating duty and requires different levels of diligence by directors for different board topics, depending on the significance and potential impact of each topic to the company.

Because cyber risk can be one of the most important risks to the company, the board's level of oversight should be commensurate with that high level of risk. To fulfill their duty of care, directors do not need to become cyber experts, but they should ask sufficient questions, require sufficient information, and receive sufficient comfort from experts to be satisfied that the unique cyber risks of the company are being reasonably addressed in ways consistent with legal requirements, industry best practices, and the reasonable expectations of company constituents.

SEC "Disclosure Guidance"
In October 2011, the Securities and Exchange Commission's Division of Corporation Finance released "CF Disclosure Guidance: Topic No. 2–Cybersecurity," which summarizes the SEC's views regarding a company's disclosure obligations relating to cybersecurity risks and incidents. It does not change existing disclosure law but merely explains the SEC's interpretation of how existing law relates to the evolving topic of cybersecurity.

The primary focus of the "Disclosure Guidance" is to assist companies in determining whether they should disclose information concerning cybersecurity and cyber incidents to investors. The ultimate question is whether known cyber incidents or the risk of potential incidents is reasonably likely to have a material effect on the company's operating results or financial condition. Factors that the SEC suggests a company consider in determining what, if anything, should be disclosed relating to cyber risk include:

- Frequency and severity of prior cyber incidents.
- Probability of cyber incidents' occurring.
- Potential costs and consequences of cyber incidents.
- Adequacy of preventative actions taken.
- Risk level of threatened cyber attacks.

If disclosure is required, the "Guidance" discourages boilerplate disclosures and encourages specific disclosures identifying the portion of the company's operations susceptible to the disclosed cyber risk, any material cyber incidents the company has experienced and the consequences of those incidents, and risks from cyber incidents that may remain undetected for an extended period.

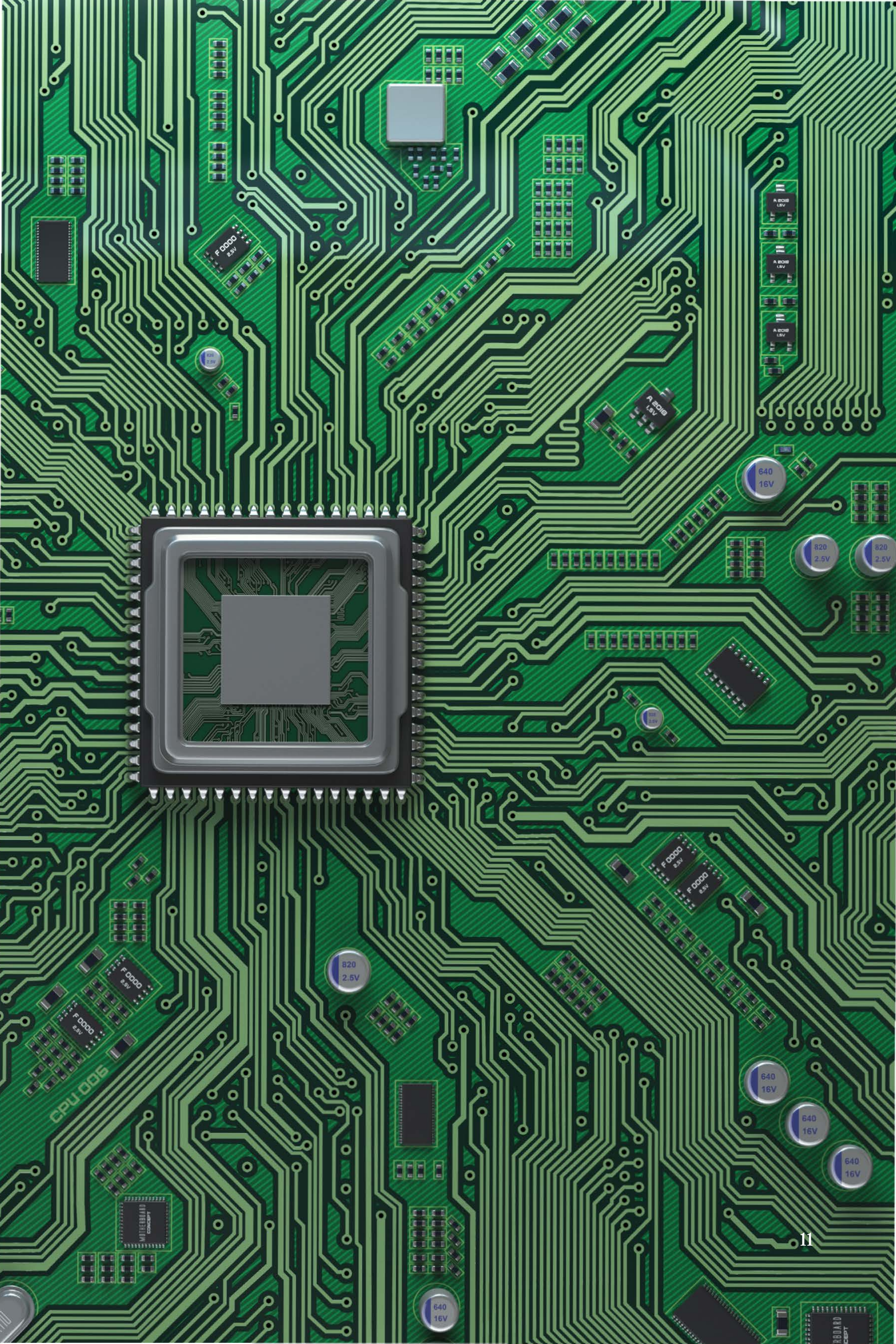
FTC "Red Flags Rule"
The so-called "Red Flags Rule" (16 CFR 681) issued by the Federal Trade Commission (effective December 31, 2010) requires a wide variety of companies to adopt identity theft protection programs that (i) identify warning signals that should alert a company to the risk of identity theft and (ii) detect, mitigate, and deal with identity thefts when they occur. The Rule states that a company's board of directors or an appropriate committee designated by the board must approve the Identity Theft Protection Program.

The Rule applies to financial institutions and "creditors," broadly defined as "any person who regularly extends, renews or continues credit." A wide variety of entities that extend credit or give credit terms are arguably subject to the Rule, perhaps including, for example, companies that permit deferred payments by customers.

Under the Rule, larger and higher-risk entities must have more comprehensive identity theft protection programs than smaller or lower-risk entities. These programs must include the establishment, testing, and deployment of an effective program to identify and act upon “red flags” that alert companies to identity theft or the potential for identity theft. Merely adopting a program without proactive enforcement and oversight does not satisfy the Rule. Directors should carefully review the identity theft protection program recommended by management and should, before approving that program, assure themselves that the program is reasonably robust, is sufficiently tailored to the unique circumstances of the company, is properly funded and staffed, and will be periodically reviewed by senior management and the board for effectiveness.

Critical Infrastructure Cyber Guidelines

In February 2014, the National Institute of Standards and Technology (NIST) issued its “Framework for Improving Critical Infrastructure Cybersecurity,” pursuant to the directive of President Obama in Executive Order 13636. The “Framework,” which is primarily directed to senior management and directors of companies in “critical infrastructure” industries, is a set of standards, methodologies, procedures, and processes to use in developing an enterprise-wide risk management approach to cybersecurity. The “Framework” is organized around five core activities that directors and senior management should address when dealing with cybersecurity risk: identify, protect, detect, respond, and recover.


640
16V
820
2.5V
CPU 006

The "Framework" is voluntary, and its stated purpose is not to replace existing sector standards or add an unnecessary layer of regulation to existing standards and practices. However, at least some modified version of the "Framework" will likely be incorporated into many commercial contracts for critical infrastructure. Plus, plaintiffs' lawyers will likely contend the "Framework" reflects a minimum standard of care for cybersecurity.

Critical infrastructure is broadly defined in the "Framework" as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on cybersecurity, national economic security, national public health and safety, or any combination of those matters." Industries specifically referenced as having critical infrastructure include financial services, energy, communications, health care, utilities, transportation, and food and agriculture.

Industry-Specific Standards

Several industries that possess sensitive consumer information are subject to additional specific regulatory standards. For example, under the Gramm-Leach-Bliley Act (1999), financial institutions are required to establish appropriate standards to safeguard a customer's personal financial information. Directors and officers of financial institutions can be personally liable for civil penalties of up to $10,000 for each violation if they fail to comply with this requirement. Similarly, the Payment Card Industry Security Standards Council adopted a list of cybersecurity standards (PCI-DSS) applicable to any company that processes credit cards, such as retailers and financial institutions. These standards include the need to "develop and maintain secure systems and applications" and to "track and monitor all access to network resources and cardholder data."

The health care industry is also subject to unique cybersecurity requirements. The Health Insurance Portability and Accountability Act (HIPAA) requires a company to protect and maintain the confidentiality of protected health care information that is created, received, maintained, or transmitted by the health care organization and to protect against any reasonably anticipated threat or hazard to the security or integrity of health care information. Pursuant to the Health Information Technology for Economic and Clinical Health Act, HIPAA requirements apply to any organization or individual who handles protected health care information, thereby imposing these cybersecurity requirements on a wide variety of companies outside the health care industry.

State Notification of Data Breach

Almost every state has a data breach law that requires a company to notify the state of a data breach. These laws vary as to what types of breaches must be reported, to what state authority notices must be submitted, the amount of information to be included in notices, and which state has jurisdiction over each breach. A cyber risk management program should include information about the requirements and applicability of state laws.

Loss Mitigation

Directors should have a high level of understanding in all aspects of the company's cyber risk. But in light of the highly technical and rapidly changing nature of cyber risk, directors should resist the temptation and the urging by some parties to become too enmeshed in cyber risk details. As with their response to any other company risk, directors shouldact as a reasonable oversight function without actively managing the risk. Balancing appropriate proactive oversight (including an adequate understanding of the risk) against inappropriate management of risk is a fundamental challenge for directors and an important distinction.

Director involvement in a company's risk management practices is obviously not a new idea. Directors are expected to reasonably manage and guide the company, which includes making informed decisions regarding acceptable levels of risk and prudent management of risk exposures. In recent years, many companies have enacted some type of enterprise risk management (ERM) program to address financial, reputational, operational, and strategic risks. Cyber risk should be addressed in the context of a company's overall ERM program, although the high severity and uniqueness of cyber risk justify special attention by directors.

It is particularly important to develop a corporate culture that continuously educates all employees throughout the company (as well as third parties with access to the company's information technology) regarding the importance and terms of the company's cyber risk management program. Directors, their assistants and families should have additional cyber security training.

The following summarizes different components of an effective risk management program to reduce the likelihood of, and the potential harm from, a future cyber incident.

Management Responsibility for Cyber Risk
Directors should ensure that a knowledgeable senior officer with cross-departmental authority is responsible and accountable for creating, implementing, enforcing, and updating an integrated, companywide cyber risk management program. Someone other than the Chief Information Officer is preferred to avoid the perception of a silo mentality. That senior executive officer should report directly to the CEO or CFO and have regular contact with the board or a designated committee of the board.

A companywide management team, or incident response team, should work with the designated senior executive officer. The team should include representatives from IT, legal, risk management, public relations, compliance/audit, finance, and human resources. This team should have primary responsibility for the company's cyber risk management program and should have access to sufficient personnel and funds to properly discharge its functions.

Directors should have high confidence in the authority of, the internal respect for, and the cyber and risk management knowledge and experience of this senior management team. If a high level of confidence does not exist, directors should consider retaining qualified consultants to assist in the risk management program responsibilities.

Identification and Evaluation of Most-Significant Cyber Risks

Directors should identify and understand the company's greatest cyber risks so they can determine whether those risks are being anticipated, managed, and mitigated adequately. The analysis includes both the areas of company technology that are most vulnerable to a cyber incident and the scenarios that can create the greatest harm to the company and its constituents.

This risk assessment should go beyond the company's own technology platforms. Other organizations with which the company transacts business or acquires can have cyber vulnerabilities that the company inherits. In fact, some of the most severe cyber incidents have occurred through vulnerabilities in the IT systems of companies' vendors and suppliers. Therefore, the degree of interconnecting between the technology platforms of a company and its suppliers, vendors, affiliates, and customers, and the quality of those third parties' cyber controls and policies, should be considered part of this analysis. Particular attention should be directed to third-party service providers to whom the company outsources IT or business processes and to international firms interconnected with the company. Companies that use external networks or public "clouds" to store or process data should consider the risks that practice creates.

Merger and acquisition activities should be thoroughly audited from a cyber risk standpoint before being integrated into the company's systems. Frequently, acquisitions occur on accelerated timelines and without complete due diligence, which opens the door to increased cyber risk. Integration of two entities' IT systems should occur only after a thorough audit of the acquired company's cyber risk profile, despite strong business pressure for a quicker integration.

Directors should receive periodic reports summarizing the extent to which third-party service providers have access to or are interconnected with the company's network applications and information, what cyber risk audits these service providers undergo, what agreements are in place with service providers to address these risks, and how the risks that arise from the service providers' downstream providers are being addressed. Similarly, how the company manages cyber risks arising from employees' cell phones, laptops, and other remote devices should be included in the discussions with directors.

In addition to external threats, directors should understand how internal cyber risks are being controlled. Disgruntled, dishonest, or poorly trained employees may obtain access to the company's most sensitive IT platforms and data and create enormous harm. Directors should understand how this risk is being managed with respect both to current and former employees.

Directors should also understand what level of cyber risk exists with respect to the company's most important data and processes. For example, directors should discuss with management what the company's most valuable or critical data assets are and how vulnerable those assets are to a cyber incident. In other words, directors should generally understand the company's vulnerability to and protection from the likeliest cyber incidents as well as less likely but highly impactful cyber incidents.

Periodic Assessment of the Cyber Risk Management Program and Its Effectiveness

Cyber risk constantly changes. Hackers are becoming increasingly sophisticated, state-of-the-art cyber defenses evolve frequently, and companies' critical data assets and cyber risk profiles can quickly change. Therefore, directors should regularly discuss with their company's designated cybersecurity officer the present cyber risk environment for the company and its industry, the status of the company's cyber risk management program, and other related topics. Directors should seek to identify through these discussions the issues that most trouble the cybersecurity officer, what new vulnerabilities exist, what new responsive strategies are being adopted, and whether the officer is encountering any barriers, such as inadequate resources or internal conflicts, to effectively managing cyber risk. These discussions with the appropriate board committee should occur quarterly, and it is prudent to brief the entire board at least semiannually (more often if situations warrant).

Directors should also use these discussions to evaluate the quality of the cybersecurity officer. Is that person knowledgeable, credible, and proactive? How well does that person stay current with industry risks and cyber management trends? Has that person established an ongoing relationship with the FBI and other appropriate law enforcement authorities responsible for cybercrime? Has that person earned the respect and cooperation of other senior officers and employees?

In addition to these broad discussions, the board or a designated committee of the board should regularly receive a dashboard of important metrics that disclose the volume, nature, and consequence of reportable cyber incidents as well as cyber risk management activities. These metrics should include information about significant intrusion attempts as well as actual significant cyber incidents. The goal of this dashboard reporting is to enable directors to assess the company's actual risk experience and its major risk management activities and to document the extent and frequency of the board's cyber oversight activities.

To evaluate the effectiveness of the cyber risk management program, frequent testing of that program through mock attacks and other exercises and through a periodic audit by independent outside cyber experts is recommended. The results of these tests and audits should be presented to the board.

Directors should also confirm that all employees participate in an ongoing cybersecurity education program that sensitizes employees to high-risk activities to avoid and educates employees on dos and don'ts prior to and after a cyber incident occurs. Employees at all levels within the company and in a variety of business units need to be prepared to respond within hours, if not minutes, to a detected cyber event. A rapid, effective response will occur only if all employees are thoroughly trained. An inadequate or a delayed response to a cyber event can greatly expand the harm the event causes.

Director Oversight

Different boards maintain different structures for implementing their cyber risk oversight functions. To ensure adequate attention and in-depth analysis, most boards delegate this responsibility to a board committee. A growing number of boards now have an enterprise risk committee that oversees company management of a wide variety of risks–such a committee could be ideal for oversight of cyber risk as well. In the absence of a risk-specific committee, most boards assign this oversight function to the audit committee. In any event, the full

board should be informed about and comfortable with the company's cyber risk management program if cyber risk is identified as a significant threat to the company and its constituents.

For companies with particularly acute cyber risks, the board should consider the benefit of directly retaining an outside expert for advice so directors are not exclusively dependent on input from the people who designed and implemented the cyber risk program. In extreme cases, the board could include a cyber expert as a director to further enhance its independent oversight function in this area.

Adequate Company Resources
Directors should confirm that the company's cyber risk management program has adequate staffing and budget. An exemplary written plan is meaningless if it is not properly implemented, enforced, monitored, tested, and updated, which requires significant resources.

Some metrics that the board can review to determine the adequacy of the company's resource commitment to cybersecurity include the following:

- How many dollars per employee are spent for cybersecurity?
- What percentage of the IT budget is the cybersecurity budget?
- How is the cybersecurity budget allocated among different departments or business units?

The board should compare these metrics with industry statistics to evaluate the adequacy of the company's resource commitment. Reasonable budget numbers can vary significantly depending on the industry. For example, companies that possess sensitive customer information or process large amounts of money (such as financial institutions, insurance companies, retailers, or health care organizations) or that are involved in critical infrastructure (such as utility, energy, communications, transportation, or food and agriculture companies) should devote a higher percentage of resources to cybersecurity than companies with lower cyber risk (such as manufacturing companies).

The directors' resource review should not be limited to budget issues. The number and quality of personnel devoted to this area is equally important. Having trained and knowledgeable employees devoted full time to cybersecurity is far more desirable than using more general risk management employees with little if any detailed cybersecurity training.

Management and the board must obviously balance the demand for more resources against the reality that only limited resources are available. When evaluating whether the appropriate balance exists within the company, directors should consider the value of the assets being protected, the level and magnitude of cyber risk being managed, and other initiatives being impaired by directing resources to cybersecurity instead.

Incident Response

Once a significant cyber event occurs, directors should address an additional list of questions and concerns. It is very important that directors anticipate and prepare for this eventuality so they can react in a thoughtful and decisive manner. Similar to the role of directors with respect to creating and implementing the cybersecurity risk management program, the role of directors after a significant cyber event occurs should continue to be in the nature of oversight rather than direct management. Following are various loss prevention suggestions for directors in this context.

Investigation

The most important step immediately following discovery of a significant cyber event is to understand the scope and impact of the event. Without interfering with management's response efforts, directors should ask questions and receive information regarding the following issues:

- What data or assets were stolen or harmed?
- Have any company operations been compromised?
- What is the likelihood that any company constituents have been or will be harmed?
- Have the company's crisis response and cyber risk management programs been implemented? Are they effective?
- Is the company confident that the intrusion has terminated?
- What steps are being taken to minimize the increased vulnerability the event caused?
- Have there been any gaps identified in prior incidents?

After the immediate crisis has subsided and the company's investigation has matured, directors should inquire about lessons to learn from the experience that can improve the company's efforts to avoid future events and mitigate future harm.

Disclosures

Directors should focus particularly on disclosure issues following a significant cyber event. Inaccurate or misleading disclosures could aggravate the problem and result in claims against directors.

Difficult disclosure issues can arise in this context. When should disclosures occur? To whom should disclosures be made? What information should be included in disclosures? These decisions should be made only after senior management has received input and advice from appropriate internal staff and qualified external legal and forensic advisers.

Following are fundamental disclosure guidelines that can assist directors in evaluating the adequacy of the company's disclosure decisions and practices regarding a significant cyber event.

Use experienced spokespeople.

Disclosures should be made through a relatively small number of clearly identified company spokespeople who are experienced and schooled in disclosure issues. All company employees should be instructed to forward any inquiries to an appropriate person or department within the company and should be prohibited from making any external comments about the cyber event without prior approval. The chain of command for approval of company disclosures should be well-defined and relatively short so that decisions can be made quickly if necessary.

Implement document retention policies.
Facts and evidence relating to the cyber incident should be preserved for later reference, particularly if investigation or litigation is expected or pending. The company should be able to establish at a later date the source and veracity of the information contained in each disclosure and the reasons additional information could not be disclosed. In addition, records of all disclosures and external communications relating to the event should be preserved.

Insurance

Insurance coverage for the company and its directors is an important consideration when evaluating cyber risk. Two types of insurance policies should be primarily considered: (i) the company's standard directors and officers (D&O) liability insurance policies and (ii) the standard cyber insurance policies. Companies concerned about cyber issues should purchase both types of policies because each policy covers different but equally important cyber risks. Both types of policies are briefly described below.

D&O Liability Insurance

D&O liability insurance policies generally afford coverage for any type of claim made against directors and officers relating to any type of incident or wrongdoing, subject to a few standard exclusions and coverage limitations. D&O policies usually do not include a cyber-specific exclusion, in which case any type of cyber-related claim brought by any type of plaintiff against insured directors and officers will generally be covered, unless another type of exclusion applies. However, D&O policies typically afford little if any coverage for most claims against a company or for loss incurred by the company. Therefore, the company should purchase a different type of policy to cover its cyber risk.

The exclusions contained in a standard D&O liability insurance policy will rarely apply to a claim against individual directors and officers simply because it is cyber-related, although the terms of each specific policy should be carefully reviewed in this regard. The following summarizes four coverage limitations that may have unique applicability to cyber-related claims, although these limitations may not have applicability in all cyber-related D&O claims.

- Property Damage Exclusion. This standard exclusion typically eliminates coverage for any claim for “damage to or destruction of any tangible property, including loss of use thereof.” It is important to note that the exclusion applies only to a claim in which the plaintiff seeks recovery for the property damage and typically does not apply to a claim by shareholders or regulators who do not directly incur the property damage. Most cyber incidents do not directly cause damage to a claimant’s tangible property and therefore do not trigger this exclusion.
- Invasion of Privacy Exclusion. Many D&O liability insurance policies contain an exclusion that eliminates liability for any claim for “violation of any right of privacy.” Like the property damage exclusion, the invasion of privacy exclusion usually applies only to a claim by a plaintiff whose privacy was invaded because of a violation of his or her legal right of privacy. Such a claim against directors and officers in the cyber context has so far been rare.
- Conduct Exclusion. Most standard D&O liability insurance policies contain an exclusion that eliminates liability for any claim based on or arising out of deliberately fraudulent or criminal conduct if a final adjudication establishes that such egregious wrongdoing occurred. However, the exclusion typically applies only to the insured director or officer who committed the deliberate fraud or criminal wrongdoing and does not apply to any other director and officer who may be sued because of the fraudulent or criminal conduct of another insured. Therefore, even if a director, an officer, or an employee of the company participates in or causes a fraudulent or criminal cyber event, other insured directors and officers typically would not lose their coverage.

- Penalties Exclusion. Many D&O liability insurance policies contain an exclusion for fines or penalties assessed against an insured director or officer. However, that exclusion typically does not apply to defense costs.

Because of the limited scope of these and other potentially applicable coverage limitations for cyber-related claims, insured directors and officers may have coverage under the company's standard D&O liability insurance program for cyber-related claims.

Cyber Insurance Policies
The other standard insurance policies a company purchases (including its general liability and property policies) likely afford limited, if any, insurance coverage for the company's losses arising from a cyber event. Cyber insurance policies are available to fill that gap in coverage and is specifically tailored for a company's cyber-related risk.

Cyber insurance policies vary greatly among insurers, but they frequently cover both claims against the company (and its directors, officers, and employees) by third parties ("third-party coverage") and losses directly incurred that arise from a wide variety of cyber risks ("first-party coverage").

The third-party coverage usually applies to defense costs, settlements, judgments, and other loss incurred by the insureds in claims by customers and other third parties who seek recovery of damages caused by the theft, loss, or misuse of the plaintiff's personal data or other harm the cyber incident caused.

The first-party coverage in these policies reimburses the company for various losses or expenses directly incurred by the company as a result of the cyber event, including customer notification expenses, credit and identity theft monitoring costs, business interruption losses, cyber extortion, costs to replace or repair damaged systems or data, forensic investigation costs, loss from theft of money or digital assets, and public relations costs.

Cyber insurance policies are complex, vary greatly, are still evolving, and, in some circumstances, can be tailored to a company's unique risk management needs. Therefore, a company should use an experienced, knowledgeable adviser with cyber insurance expertise to evaluate the benefits from, the reasonable costs for, the best available terms of such a policy.

About The Author

Dan A. Bailey, Esq., a member of the Columbus, Ohio, law firm Bailey Cavalieri LLC, is one of the nation's foremost experts on matters relating to directors and officers (D&O) liability, litigation, and insurance. He and his firm have represented or served as a consultant to a wide variety of directors and officers, corporations, insurance companies, insurance brokers, and law firms around the United States regarding D&O matters.

A frequent speaker at seminars throughout the country regarding D&O liability and insurance, Mr. Bailey is also the coauthor (with William E. Knepper) of *Liability of Corporate Officers and Directors*, and he has written dozens of articles on the subject.

Mr. Bailey received his B.S. degree in business administration *cum laude* from Bowling Green State University in 1975 and was awarded a Juris Doctorate degree with honors from the Ohio State University School of Law in 1978. He is a member of numerous honoraries and was selected for inclusion for *Who's Who in America*.

Chubb. Insured.℠

Updated 02/2023