7 tactics for winning the cyber war

Battle strategies for directors and officers

McDonald Hopkins

A business advisory and advocacy law firm®

Attorney **Insight.** Business **Foresight.®**

Introduction

"Victorious warriors win first and then go to war, while defeated warriors go to war first and then seek to win."

Sun Tzu's advice from the centuries-old "The Art of War" still rings true today. As you collect more personal and sensitive customer and commercial data, you must proactively prepare to defend yourself against – and win – the cyber war. The attacks can come on multiple fronts: external threats, intentional misappropriation by rogue employees, data accidentally lost or misplaced and vendor negligence. And per the 2015 Ponemon Institute Cost of Data Breach Study, the risks could not be higher:

- The average cost of a data breach is $6.5 million – $217 per compromised record
- The average cost for crisis services, including forensics, notification, and legal guidance is approximately $370,000
- The average cost for legal defense is $700,000
- The average cost for legal settlement is $560,000
- Post data breach costs average $1.64 million
- Lost business costs per data breach average $3.7 million

The 2014 Ponemon study revealed equally important insight:

- 62 percent of consumers said breach notification decreased trust and confidence in the organization
- 15 percent would terminate their relationship with the notifying company (39 percent would consider terminating)
- 94 percent believe an organization reporting a breach is solely to blame for the breach

94%

believe an organization reporting a breach is solely to blame for the breach

When your company is the victim of a cybersecurity breach – or if you have a substandard cybersecurity program – there is a lot at stake. And the laws surrounding data breaches are quickly evolving, too.

As the number of data breaches grows, whether an actual injury (beyond the fear and threat of future identity theft and other potential cyber harm) is required for standing continues to be a critical mass and class litigation question. In a departure from previous decisions requiring an actual injury be present to create Article III standing, in *Remijas v. Neiman Marcus Group, LLC*, No. 14-3122 (7th Cir. July 20, 2015) the Seventh Circuit Court of Appeals determined that the plaintiff class "should not have to wait until hackers commit identity theft or credit-card fraud in order to give the class standing, because there is an 'objectively reasonable likelihood' that such an injury will occur." Further, "at this stage in the litigation, it is plausible to infer that the plaintiffs have shown a substantial risk of harm from the Neiman Marcus data breach … presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identity." The Seventh Circuit's finding that likely future harm is sufficient for standing to sue is significant as it has arguably reduced the standing barrier and more consumer data breach lawsuits will likely survive initial dismissal attempts and go on to class certification – increasing risks for entities and their boards.

Cyber attacks also directly threaten business continuity and can have a disastrous effect upon valuation. Your reputation can also take a hit, which in turn negatively impacts share value and potential business sale prices. In contrast, a proactive, enterprise-wide cybersecurity program overseen by your board can have a positive impact on sale price and business valuation. Many boards now consider cybersecurity when conducting due diligence or, in the case of equity funding, considering investments.

Cybersecurity is clearly not just an IT issue, but a corporate strategy issue that affects everything from the bottom line to top level executives and directors.

What many board members don't realize is that in the face of a cyber attack, they can find themselves in the crosshairs of shareholder derivative action alleging breach of fiduciary duty and/or regulatory enforcement actions. In fact, the next generation of cyber attacks has been targeting individuals with privileged access to financial data, systems control, or root access – specifically officers, employees like CFOs, system and database administrators, and board members. The cyber attackers gather card data or personally identifiable information and then move throughout an organization.

Unfortunately, many officers and directors do not fully understand the scope and magnitude of the issues their company faces, nor do they ensure that cybersecurity efforts integrate with overall business strategy. A recent FTI Consulting study noted that 52 percent of directors ranked IT strategy and risk as an issue for which they need better information. Tellingly, a National Association of Corporate Directors survey of over 1,000 directors revealed that only 11 percent of board members felt they had a "high level" of cybersecurity knowledge.

Historically, courts enforced a high threshold for oversight failure before finding directors liable for breach of fiduciary duty claims. A 2006 study published in the Stanford Law Review indicated that in the 25 years leading up to the study, only 13 cases were found where directors made out-of-pocket payments not covered through D&O insurance policies. While history might suggest that personal financial loss to directors resulting from a cyber attack may not be likely, the reputational risk and indirect financial implications of losing a board seat (see, Institutional Shareholder Services' recommending "no votes" for several of Target, Inc.'s directors) will undoubtedly get the attention of directors in other enterprises. Clearly, any underestimation of the scope of risk and implications associated with cybersecurity and data privacy issues and claims is a mistake.

Based on existing regulatory guidance, expert analysis, and case law, in order to protect your officers and directors from risk and liability you should be asking the following critical questions:

1. How do cybersecurity issues affect officer and director fiduciary duties and potential liabilities?
2. What does your board need to know about the company's cybersecurity protocols and procedures?
3. Are your company's critical cyber assets identified and properly protected?
4. Has your board created cybersecurity committees and/or assigned clear roles and responsibilities within the organization for identifying, evaluating, and monitoring cybersecurity incidents?
5. What are your company's cyber incident response plans in the event of a cyber attack?
6. Is the company properly managing third-party vendors who have access to their cyber environment?
7. Does the company's insurance cover a cyber event?

To help your board members win first before they go to cyber war, this whitepaper is organized around helping you answer these questions. If you can't answer them, your company should seek attorneys, IT experts, or other consultants with regulatory expertise who can address any critical gaps.

1 How do cybersecurity issues affect officer and director fiduciary duties and potential liabilities?

Your directors should understand their fiduciary duties and what protection they have under the Business Judgment Rule[1]. As stated in *In re: Caremark International, Inc. Derivative Litigation*, 698 A.2d 959 (Del. Ch. 1996), they should specifically understand "a director's obligation includes a duty to attempt in good faith to assure that a corporate information and reporting system, which the board concludes is adequate, exists, and that failure to do so under some circumstances, may, in theory at least, render a director liable for losses caused by non-compliance with applicable legal standards." Under *In re: Caremark* and its progeny, a board can breach its cybersecurity duties by failing to work with management to:

- Implement a monitoring, compliance and risk management program
- Oversee and test the monitoring, compliance and risk management program
- Investigate possible violations once the board has actual or constructive notice of compliance and risk management issues (through whistle-blowers, formal and informal complaints, regulatory inquiries, etc.)

Courts and regulators are employing stringent standards and specifically analyzing how boards are identifying, assessing, and addressing cyber risk.

Duty to implement, oversee and test a monitoring, compliance, and risk management program

With respect to cybersecurity issues, courts and regulators are employing stringent standards and specifically analyzing how boards are identifying, assessing, and addressing cyber risk. As a result, proper board preparedness and planning are critical to insulating your directors from liability.

In the *Palkon v. Holmes*, No. 14-CV-01234 (D.N.J.) decision, a federal district court dismissed a shareholder class action against directors, the president/CEO, and general counsel of Wyndham. The class action alleged breaches of the fiduciary duties of care and loyalty, and the wasting of company assets following three data breaches between April 2008 and January 2010 that resulted in the theft of over 600,000 customers' credit card information. The Business Judgment Rule was critical to the court's decision making. The court found the rule protected the board because the board:

- Held 14 quarterly meetings in which it discussed the cyber attacks, company security policies, and proposed security enhancements
- Appointed the audit committee to investigate the breaches. That committee met at least 16 times to review cybersecurity.
- Hired a technology firm to recommend security enhancements, which the company had begun to implement
- Had cybersecurity measures in place that had been discussed numerous times by the board prior to the security breach

While the appeal of the civil litigation was dismissed, the Federal Trade Commission conducted its own investigation with respect to these breaches, and in June 2012, filed *Federal Trade Commission v. Wyndham Worldwide Corp., et al.,* Case No. 2:13-cv-01887 (D. N.J.). On August 24, 2015, the Third Circuit affirmed in *FTC v. Wyndham Worldwide Corp.,* 14-3514 (U.S. Court of Appeals for the Third Circuit (Philadelphia)), that the FTC has the authority to police companies' cybersecurity practices. Wyndham is actively defending itself against the FTC's claims that it failed to properly secure its systems and take reasonable steps to prevent the

[1] The Business Judgment Rule is a presumption that in making a business decision, the directors of a corporation acted on an informed basis, in good faith, and in the honest belief that the action taken was in the best interests of the company. Accordingly, absent other circumstances, courts defer to such business judgment and will not review resulting business decisions.

breaches. Wyndham's directors have supported the company in its defense of the FTC; however, their fiduciary duties also required them to independently decide if the breaches were the result of negligent or reckless conduct by Wyndham's officers, which may have required the company to file its own civil action against its officers.

On the other end of the spectrum is a decision from the Third U.S. Circuit Court of Appeals. While not a cyber case, *In re: Lemington Home for the Aged*, No. 13-2707 (3d Cir. 2015) offers a cautionary tale to board members who recognize potential organizational and governance risks, but fail to address them. The Lemington Home was a nonprofit nursing home that ultimately sought bankruptcy protection and closed because of service deficiencies and financial troubles. The Committee of Unsecured Creditors filed an adversary proceeding against the CEO, CFO, and all 15 former directors, claiming breach of fiduciary duty, breach of the duty of loyalty, and deepening insolvency. In 2013, the jury awarded compensatory damages of $2,250,000; punitive damages of $350,000, individually, against five directors; and punitive damages of $1 million against the CFO and $750,000 against the CEO.

In this case, the court's fiduciary duty standards required that officers and directors perform their duties in good faith and in the best interest of the corporation with the care, reasonable inquiry, skill, and diligence an ordinary person would take under similar circumstances. In so doing, directors and officers could rely on information, opinions, reports, or statements, including financial statements prepared by others. While the officers and directors were protected by the Business Judgment Rule, they were not considered to have acted in good faith when they had knowledge of a situation that would cause their reliance to be unreasonable.

The Third Circuit found evidence that supported the jury's findings that the directors did not exercise reasonable care by allowing the named officers to remain in their roles, and that fiduciary duties were breached when the board failed to take action to remove them once the results of their mismanagement were clear. It was known that proper financial records were not maintained, that the facility had numerous service deficiencies, and that several independent reports documented administrative shortcomings. Thus, "[t]his [was] not a case where directors, acting in good-faith reliance on 'information, opinion, reports or statements' prepared by employees or experts, made a business decision to continue to employ an Administrator whose performance was arguably less than ideal..." Rather, the "directors in this case had "actual knowledge of mismanagement, yet stuck their heads in the sand in the face of repeated signs that residents were receiving care that was severely deficient."[2]

In re: Lemington Home for the Aged is a very instructive fiduciary duty case and, like *Palkon*, may be an indication of how courts will analyze future cybersecurity cases. *In re: Lemington Home for the Aged* is completely consistent with the seminal analysis in *In re: Caremark,* which noted that "only a sustained or systematic failure of the board to exercise oversight—such as an utter failure to attempt to assure a reasonable information reporting system exists—will establish the lack of good faith that is a necessary condition to liability." However, the *In re: Lemington Home for the Aged* court's exacting analysis subjected the officers and directors to immense personal liability for failure to properly identify, detect, and protect the entity from organizational risks before they occurred, and for failure to properly respond when such failings were exposed.

From *Palkon,* you can learn how your officers and directors can protect themselves and your organization from liability. From *In re: Lemington Home for the Aged,* you get a preview of what can happen if proper cyber risk management and security protocols are not put in place and consistently monitored by management and the board.

Investigations should begin as soon as possible after a triggering event.

[2] The Third Circuit also found that fiduciary duties were breached and, recognizing the "tort of deepening insolvency," that the defendants deepened the insolvency of the institution and damaged any financial viability for the organization. Accordingly, it affirmed the liability findings and the punitive damages awards against the officers, but vacated the award of punitive damages against the directors stating that the requisite "malice, vindictiveness and a wholly wanton disregard of the rights of others" could not be established for punitive damages.

Duty to properly investigate and address cyber incidents

As the scope of what cybersecurity programs must cover grows, your board must oversee management's development of internal investigation and breach response protocols to fully discharge their fiduciary duties.

Generally, an investigation is an appropriate response to:

- Notice of a data breach or cyber attack
- Government investigations and enforcement actions
- Allegations of employee or company wrongdoing
- Whistle-blower allegations related to data privacy or cybersecurity
- A lawsuit against the company

Investigations should begin as soon as possible after a triggering event. While an internal legal or compliance department can undertake such investigations, they are best handled by independent, outside counsel for two reasons:

1. Use of outside counsel can cement attorney-client privilege, protecting critical and confidential information and analysis from discovery.
2. Engaging outside counsel with other advisors can help support invocation of the Business Judgment Rule.

Once on notice of compliance and/or risk management issues (either constructively or actually), if your board conducts a proper internal investigation and determines in good faith no further action is warranted, the Business Judgment Rule should protect their decision. However, if there is no formal process and/or only a cursory internal process is utilized, the Business Judgment Rule protection may not apply as "the presumption created by the Business Judgment Rule can be rebutted only by affirmative allegations of facts which, if proven, would establish fraud, bad faith, overreaching or an unreasonable failure to investigate material facts." (*Berg & Berg Enterprises v. Boyle*, 178 Cal. App. 4th 1020, 1046)

Engaging outside counsel to conduct high-stakes investigations not only provides attorney-client privilege protection, it is also concrete indicia of good-faith investigation, creating a shield for your board and an obstacle for litigants to overcome.

Engaging outside counsel to conduct high-stakes investigations not only provides attorney-client privilege protection, it is also concrete indicia of good-faith investigation, creating a shield for your board and an obstacle for litigants to overcome.

2 What does your board need to know about the company's cybersecurity protocols and procedures?

When addressing the level of cybersecurity awareness expected from board members, Securities and Exchange Commission Commissioner Luis Aguilar observed in June 2014:

> *When considering the board's role in addressing cybersecurity issues, it is useful to keep in mind the broad duties that the board owes to the corporation and, more specifically, the board's role in corporate governance and overseeing risk management. It has long been the accepted model, both here and around the world, that corporations are managed under the direction of their boards of directors.*
>
> *Good boards also recognize the need to adapt to new circumstances — such as the increasing risks of cyber-attacks. To that end, board oversight of cyber-risk management is critical to ensuring that companies are taking adequate steps to prevent, and prepare for, the harms that can result from such attacks. There is no substitution for proper preparation, deliberation, and engagement on cybersecurity issues. Given the heightened awareness of these rapidly evolving risks, directors should take seriously their obligation to make sure that companies are appropriately addressing those risks.*

Commissioner Aguilar also noted that the recently created National Institute of Standards and Technology (NIST) Cybersecurity Framework creates a template that corporations, directors, and officers can adapt to their organizational needs:

> *The NIST Cybersecurity Framework is intended to provide companies with a set of industry standards and best practices for managing their cybersecurity risks. In essence, the Framework encourages companies to be proactive and to think about these difficult issues in advance of the occurrence of a possibly devastating cyber-event. While the Framework is voluntary guidance for any company, some commentators have already suggested that it will likely become a baseline for best practices by companies, including in assessing legal or regulatory exposure to these issues or for insurance purposes. At a minimum, boards should work with management to assess their corporate policies to ensure how they match-up to the Framework's guidelines – and whether more may be needed.*

To enhance cyber preparedness, your board should understand that the NIST Cybersecurity Framework encourages organizations to incorporate these core principles into their cybersecurity plans:

- **Identify:** Develop an organizational understanding required to manage cybersecurity risk to systems, assets, data, and capabilities
- **Protect:** Develop and implement appropriate safeguards to ensure delivery of critical infrastructure services and ensure the proper monitoring and control of third-party vendors
- **Detect:** Develop and implement the appropriate activities to identify and avoid cyber events
- **Transfer:** Develop and implement an appropriate insurance program that deals with cyber and privacy events
- **Respond:** Develop and implement the appropriate activities to respond to a breach or other cyber event
- **Recover:** Develop and implement appropriate plans to maintain resilience and restore any capabilities or services that were impaired by a cybersecurity event

Regardless of how these duties are fulfilled, your board should have a high-level understanding of your cyber risks. Then, they should work with management to understand and oversee the systems in place to identify, manage, and mitigate cybersecurity risks, and respond to cyber events. All of this means that you need to take a deliberate approach in identifying, assessing, and addressing relevant cyber risks.

Experienced legal counsel working with IT experts is the best option to conduct this type of analysis. They can ensure appropriate regulatory interests are understood and proactively addressed. This also makes it possible for you to protect your discussions with the attorney-client privilege. It is wise to engage directors who have specific knowledge of cybersecurity regulations and programs so they can better inform and guide the entire board. To demonstrate that your board has properly discharged their duties, they must work with management to ensure the assembly of proper teams and prepare plans to prevent and respond to any cyber breaches.

Regardless of how these duties are fulfilled, your board should have a high-level understanding of your cyber risks.

3 Are your company's critical cyber assets identified and properly protected?

To minimize cyber risk, it is important to have a clear understanding of what critical information and assets you possess, how they are maintained, and what can be accessed. This includes:

- **Personally Identifiable Information (PII)**
  - Social Security number
  - Driver's license number
  - Credit/debit card numbers
  - Passport number
  - Banking records
  - Date of birth
  - Mother's maiden name
- **Protected Health Information (PHI)**
  - Medical/status records
  - Provision of healthcare
  - Payment for healthcare
- **Business information**
  - Customer/prospect lists
  - Trade secrets
  - Business plans and strategies
  - Employee lists

Analyze what internal and external threats to your critical cyber assets exist.

Next, you must analyze what internal and external threats to your critical cyber assets exist. Primary forms of data theft include:

- **Physical loss:** Stolen or lost laptop, smartphone, thumb drive, or other mobile device containing personal information or other sensitive data, and hardcopies.
- **Database/server breach:** Unauthorized person accesses or hacks into a data server that stores personal or other sensitive data.
- **Stolen data by otherwise authorized users:** Employee or other person with access downloads or sends personal or sensitive data to another unauthorized location for an improper purpose.
- **Vendor/third-party breach:** Negligence, physical loss, database/server breach, or stolen data at a vendor or third-party administrator's (licensee) location or server.

Critical questions to consider include:

- Do some employees have access to more data than is appropriate to their position?
- Does the manner of transfer subject data to outside threats (hacking, destructive malware, theft of online credentials, misuse of the Internet)?
- Do third-party vendors have inappropriate access to data infrastructure?

Understanding such threats will enable your board and management to deploy resources.

4 Has your board created cybersecurity committees and/or assigned clear roles and responsibilities within the organization for identifying, evaluating, and monitoring cybersecurity incidents?

Your board should have a general understanding of critical cybersecurity issues and work with management to ensure consistent staff training and ongoing monitoring. Consider appointing officers and directors with cybersecurity expertise, and creating specific board committees to address data privacy and cybersecurity issues. Follow the *Palkon* example – engaged board members and committees can help cement the Business Judgment Rule protections. And learn from the mistakes in *In re: Lemington Home for the Aged* – a perfect plan is useless if it is simply in a drawer.

Your board should have a general understanding of critical cybersecurity issues and work with management to ensure consistent staff training and ongoing monitoring.

The hallmarks of truly effective cyber risk governance strategies include:

- **Defined roles for directors and management.** Systematically defining responsibilities and assigning clear roles for management, board committees, and individual directors to ensure cybersecurity programs and protocols are developed and deployed cost-effectively throughout the organization.
- **Constant assessment of cybersecurity trends and threats.** To ensure Business Judgement Rule protection, it would be wise to have outside attorneys, along with key consultants, conduct regular presentations for your cybersecurity committee and entire board about the latest developing cybersecurity trends and threats and how they can specifically affect the organization. Again, incorporating outside counsel in this process can allow attorney-client privileges and protections to take hold and protect critical deliberations from disclosure.
- **Cybersecurity vigilance permeating the organization.** Employees, vendors, and partners must be continually educated to create a culture of cybersecurity.
- **Continually evolving cyber preparedness plans and controls.** Organizations must incorporate systematic threat and weakness assessments into their cyber risk management plans and modify established programs and protocols as required.

You need to review and create information security policies to protect your critical cyber assets and guard against actual and potential threats. Part of this process should be the development of critical performance indicators that will allow your executives and board to anticipate, identify, and address cyber risks. Such security controls and plans must:

- Ensure the security and confidentiality of their customer and employee information.
- Protect against any anticipated threats or hazards to the security or integrity of their customer information.
- Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.
- Ensure the proper disposal of customer information.

Tools necessary to achieve these goals can include:

- Access controls on customer information systems
- Access to the company domain and information assets controlled via logon and password
- Access restrictions at physical locations containing customer information
- Hardware firewalls, walls, and switches
- Encryption for all critical cyber assets
- Encryption of data that comes from other systems or third parties and sits in files before being loaded into databases (aka "data at rest")
- Mobile device/data management
- Network segmentation
- Security and network monitoring
- Device and server patch management
- Dual control procedures, segregation of duties, and employee background checks for employees with responsibilities for, or access to, customer information
- Separation of duties through controls and access. (Users are limited to what they can access and update via logons and passwords.)
- Procedures designed to ensure that customer information system modifications are consistent with the institution's information security program

Integrating cyber risk considerations and expertise into your governance framework allows you to be proactive, instead of reacting to threats and incidents as they arise. And increased board involvement can have a tangible effect on the cost of a data breach. Per the 2015 Ponemon study, board involvement decreased the average per record cost of a data breach from $217 per record to $207.

Integrating cyber risk considerations and expertise into your governance framework allows you to be proactive, instead of reacting to threats and incidents as they arise.

5 What are your company's cyber incident response plans in the event of a cyber attack?

A critical aspect of any cyber preparedness plan is the development and implementation of an incident response protocol. In fact, implementation of incident response protocols and teams decreases per record breach costs from $217 to $193. The response protocol should address unauthorized access to or use of critical information that could result in substantial harm or inconvenience to others. The components of an effective program include:

- Assessment of the nature and scope of the incident and identification of what customer information has been accessed or misused.
- Assessment of whether and when state and federal regulators should be notified once you become aware of an incident involving unauthorized access to or use of sensitive customer information.
- Notification to appropriate law enforcement authorities, in addition to filing a timely Suspicious Activity Report for certain financial institutions, in situations involving federal criminal violations requiring immediate attention.
- Measures to contain and control the incident to prevent further unauthorized access to or misuse of customer information, while preserving records and other evidence.
- Notification to customers when warranted.
- Utilization of any established business continuity plans.
- Coordination of public relations and/or crisis communication plan with counsel, consultants, and company.

Because the issue impacts almost every component of your business, and failure to properly manage can result in both long- and short-term consequences, the team should include critical board members and c-level decision makers in the following areas:

- Legal
- IT
- Risk/insurance
- HR
- Marketing
- Public relations

This group should coordinate to ensure that in the event of a cyber incident these critical steps are taken:

- Retention of attorneys to create and maintain attorney-client privilege over the response process
- Consultation with insurance brokers/carriers
- Deployment of Incident Response Team (IT, HR, legal, PR, etc.)
- Assignment of breach coordinator depending on business areas affected and IT resources implicated
- Preservation of all evidence of breach and secure IT systems using forensic specialists to contain breach
- Coordination with media consultants or internal marketing for consistent messaging
- Determination if, among other things, the Incident Response Team must:
  - Contact law enforcement
  - Send notices directly to affected individuals or work with a mail house to effectuate
    - Residence of affected individuals determines applicable notice law
    - A few states require notification of any data breach (i.e., MN)
    - Most states require notification when harm to potential victims is likely or reasonably likely (i.e., MI, OH, CA, WA)
  - Alert state attorneys general and other state and federal regulators
  - Notify appropriate reporting to credit card companies and credit reporting agencies, and decide if credit monitoring will be offered

Considering the importance of the controls, plans, and protocols, institutions with board oversight should routinely test their Incident Response Plan effectiveness and conduct tabletop exercises to evaluate existing response programs and make modifications as warranted. Institutions and boards must understand that regulator examinations should not be considered system tests. Rather, examinations should be focused on evaluating whether management and boards understand how emerging cyber attacks could affect their business. Thus, institutions should be prepared to show their regulators that they have identified and understand the risks they face. Cyber preparedness is a process, not an event.

Cyber preparedness is a process, not an event.

6 Is your company properly managing third-party vendors who have access to your cyber environment?

An essential part of assessing existing controls and plans is reviewing vendor relationships and how vendors can affect your risk profile. This process must be conducted by management and at the board of director level. You must assess the complexity of each relationship, including:

- Legal and compliance risk
- Volume of activity
- Potential for subcontractors, including the potential need for foreign support
- Technology needs
- Access to the institution systems and information

You should also specifically analyze the nature of customer interaction with the vendor and potential impact the relationship will have on consumers, including access to customers' confidential information and handling of customer complaints. Outline plans to manage these impacts. The scope and depth of vendor due diligence is directly related to the importance and magnitude of your relationship with the third-party. It is important to define, agree upon, and document expectations at the start of the engagement. Review such expectations at least annually and after a change in services. This process is also consistent with regulator expectations and should be documented in your third-party vendor management policy. Specific contract topics to be thoroughly analyzed include:

- Scope
- Performance (including setting up specific metrics and benchmarks)
- Communication plans
- Risk assessment and audit rights (perhaps with triggers for same)
- IP rights
- Data security
- Indemnification
- Response to consumer complaints
- Regulator oversight
- Insurance
- Termination

After entering into a contract with a third-party, your board should ensure that you have dedicated sufficient staff with the necessary expertise, authority, and accountability to oversee and monitor the relationship. You should also ensure that employees charged with managing third-party relationships are trained with respect to the vendor relationship and monitoring procedures. Regular site visits are useful to understand the third-party's operations and ongoing ability to meet contract requirements.

Regular site visits are useful to understand the third-party's operations and ongoing ability to meet contract requirements.

7 Does your insurance cover a cyber event?

Given the evolving D&O policies with respect to cybersecurity, directors must understand insurance policy variations and associated implications; requiring cybersecurity specialists to assess potential policy gaps, blind spots, etc. While we seem to be slowly moving towards an industry standard, gaps between first- and third-party coverage under existing policies may leave you to face uncovered losses. And specific attention should be paid to whether coverage applies to attacks over time (which occurs in many situations) as opposed to specific events.

While insurers have attempted to strengthen cyber risk exclusions within traditional policies, recent judicial decisions indicate that policyholders may still recover claims for data breach losses under policies that aren't cyber-specific in certain circumstances.

Firms should conduct a comprehensive review of their policies to determine what cyber risks are covered and which of the four typical cyber liability insurance policies should be purchased:

- **Data breach and privacy management coverage** to cover costs related to managing and resolving data breaches (investigation, breach notification, credit monitoring, legal fees, etc.).
- **Multimedia liability coverage** to address attacks on websites, media, and other intellectual properties.
- **Extortion liability coverage** to address DDoS and/or ransomware attacks.
- **Network security liability** to cover DDoS attacks and third-party data theft.

Purchasing appropriate coverage requires the completion of applications and questionnaires requesting information about a firm's data security practices and procedures, and going through this process can be helpful in providing the board a snapshot of a company's data security risks and practices. More importantly – as carriers often require that board and management will ensure that such policies and procedures continue to be in place as a condition of the coverage – boards overseeing this process should work with their attorneys to ensure that claims cannot be denied because of incomplete or inaccurate applications.

Regardless of how the courts rule, policies that do not provide specific cyber liability coverage will be of little use to companies in the wake of a data breach or other cyber attack.

Conclusion

Sadly, it is a near truism that an increase in regulation comes with increased regulatory scrutiny and litigation. Thus, it is more likely than ever that data breaches will trigger subsequent state and/or federal regulatory actions, shareholder derivative actions, and/or other claims against directors and officers. Specifically, *Remijas v. Neiman Marcus Group, LLC* should serve as a cautionary tale for all entities, their management, and boards. As data breaches increase, and individuals who have not yet suffered any actual out-of-pocket losses from a breach can sustain claims, the pool of potential plaintiffs gets bigger. Couple this with the impending increase of state and federal data breach legislation, and enterprise cybersecurity must be addressed now.

Accordingly, a shift of traditional fiduciary analysis from questions of liability and defense to questions of offensive and proactive stewardship becomes critical. To this end, companies, at the direction of the board, should consider the following actions:

- Deliberately and consistently educate directors, perhaps through outside consultants, about industry best practices and, more importantly, the company's cybersecurity policies, controls, and procedures, including:
  - Critical cyber assets and threats
  - Existing controls and programs
  - Third-party vendor management
  - Development and implementation of a cyber incident response protocol
  - Insurance coverage
  - Business continuity plans
- Appointing officers and directors with expertise in cybersecurity issues
- Creating company departments and/or board committees to be primarily responsible for data privacy and cybersecurity issues
- Conducting regular officer and director meetings to ensure that the company's expectations and processes are being diligently followed

Considering the myriad of cybersecurity risks and concerns – with directly related fiduciary duty and director liability issues – only a comprehensive, multidisciplinary approach involving the integration of multiple legal specialties and service teams can provide public, private, and nonprofit directors with the proper strategy and tactics to address cybersecurity risks while enhancing officer and director protection. Moreover, understanding and avoiding such regulatory actions will be critical to avoiding the significant costs associated with the ongoing cyber war – loss of critical cyber assets, reputational damage, potential for increased propensity for attack, fees paid to professionals to prepare and fight battles, and penalties from regulators – all can be devastating to an organization and its board.

Cyber preparedness is the only way that a board and its organization can win first and then go to (cyber)war. More importantly, cyber preparedness is the only way to ensure that cybersecurity issues do not disrupt business continuity, decrease business valuation, and adversely affect the business reputation of the company and its officers and directors. In discharging their fiduciary duties, officers and directors must take the initiative and, working with attorneys and consultants, directly address cybersecurity and ensure protocols and procedures are incorporated into a company's overall business strategy and corporate culture.

Sadly, it is a near truism that an increase in regulation comes with increased regulatory scrutiny and litigation.

McDonald Hopkins

A business advisory and advocacy law firm®

Attorney **Insight.** Business **Foresight.®**

McDonald Hopkins LLC

mcdonaldhopkins.com **Carl J. Grassi,** President

Questions about putting together your cybersecurity battle guide? Contact any one of these McDonald Hopkins attorneys.

James Giszczak
248.220.1354
jgiszczak@mcdonaldhopkins.com

David Johnson
216.348.5456
djohnson@mcdonaldhopkins.com

Richik Sarkar
216.430.2009
rsarkar@mcdonaldhokins.com

Chicago
300 N. LaSalle Street
Suite 2100
Chicago, IL 60654
312.280.0111
Richard N. Kessler

Cleveland
600 Superior Ave., East
Suite 2100
Cleveland, OH 44114
216.348.5400
Shawn M. Riley

Columbus
250 West Street
Suite 550
Columbus, OH 43215
614.458.0025
Peter D. Welin

Detroit
McDonald Hopkins PLC
39533 Woodward Ave.
Suite 318
Bloomfield Hills, MI 48304
248.646.5070
James J. Boutrous II

Miami
200 S. Biscayne Blvd.
Suite 2600
Miami, FL 33131
305.704.3990
Raquel (Rocky) A. Rodriguez

West Palm Beach
505 S. Flagler Drive
Suite 300
West Palm Beach, FL 33401
561.472.2121
John T. Metzger

***McDonald Hopkins Government Strategies LLC**
Washington, D.C.
101 Constitution Avenue NW, Suite 600 East, Washington, DC 20001 • 202.559.2600
Steven C. LaTourette

*McDonald Hopkins Government Strategies LLC is a wholly-owned subsidiary of McDonald Hopkins LLC. McDonald Hopkins Government Strategies is not a law firm and does not provide legal services.