From the Internet to the Boardroom: Health Care Director Oversight of Cybersecurity

Member Briefing, October 2015

Sponsored by the Business Law and Governance Practice Group. Co-sponsored by the Academic Medical Centers and Teaching Hospitals, Health Care Liability and Litigation, Health Information and Technology, Hospitals and Health Systems, and Physician Organizations Practice Groups.

AUTHORS

Kirstin Salzman
David Solberg
Husch Blackwell LLP
Kansas City, MO
Introduction

Massive data breaches resulting from cyber-attacks have occurred across numerous industries over the past year, captivating the nation’s attention and increasing the urgency within organizations to prioritize cybersecurity. While the frequency of cyber-attacks has risen in many industries, the security firm Websense asserts that health care providers have suffered an unparalleled increase in attacks.\(^1\) Specifically, Websense researchers reported in August 2014 that over the prior 10 months it had seen a 600% increase in attacks on hospitals.\(^2\) It also predicted that the number of cyber-attacks on hospitals would increase even more precipitously in 2015, leading the magazine *MIT Technology Review* to dub 2015 as potentially the “Year of the Hospital Hack.”\(^3\)

Reflecting on the first eight months of 2015, such ominous predictions appear to be prescient. In February, health insurance company Anthem reported that it suffered a cyber-attack that compromised the privacy of as many as 78.8 million individuals, the largest breach ever in the health care industry.\(^4\) In July, UCLA Health announced that it also was the victim of a cyber-attack that may have allowed for unauthorized access to the personal and medical information of up to 4.5 million patients.\(^5\) The adoption of electronic health records combined with the significant profitability of acquiring protected health information—stolen medical records can be sold for approximately $10 per record, which is 10 to 20 times greater than the value of a stolen credit card—ensure that cyber-attacks in the health care industry will continue to grow in the coming years.\(^6\)

\(^1\) Websense, Hack Attacks on Hospitals Jump 600% This Year, available at https://community.websense.com/blogs/websense-media-coverage/archive/2014/09/30/cnbc-hack-attacks-on-hospitals-jump-600-this-year-ceo.aspx.
\(^2\) Id.
Although many boards of directors have traditionally classified cybersecurity as an operational issue for the information technology (IT) department to handle, its weighty implications for the entire organization now require directors to consider it as a critical risk management concern. Considering that a major data breach has the potential to cripple a provider because of inappropriate destruction, or ransoming, of information by the hacker, damaged IT infrastructure, harm to organizational reputation, and harsh legal and regulatory penalties, health care directors must maintain an active role in overseeing cybersecurity. This Member Briefing first discusses the duties directors have to the organizations they serve and the potential liability they may incur stemming from a breach of the organization’s IT system. The Member Briefing then identifies key laws governing health information governance, and concludes by addressing a director’s role in cybersecurity oversight, presenting principles and questions for directors to consider as they fulfill this vital role.

**Director Liability for Cybersecurity Oversight**

**Fiduciary Duties**

Directors owe the organizations they serve certain fiduciary duties, including the duty of care and the duty of loyalty. The duty of care generally requires a director to act on an informed basis, with the amount of care an ordinarily prudent person would use in similar circumstances, and with the honest belief that the director is acting in the best interests of the organization.\(^7\) The duty of loyalty generally requires a director to act in good faith and to refrain from self-dealing.\(^8\) Derived from the duty of loyalty, the Delaware court in the case *In re Caremark International Inc.*\(^9\) also imposed a duty of oversight upon directors. This duty requires directors to ensure that a corporation has appropriate systems and controls to monitor the risks facing the corporation and to monitor the operation of those systems and controls.

---


\(^8\) *Guth v. Loft, Inc.*, 5 A.2d 503, 510 (Del. Supr. 1939).

Directors of organizations in the for-profit arena have faced derivative suits claiming that they breached their fiduciary duties by failing to properly oversee the organization’s cybersecurity efforts. For example, recently a derivative suit was filed against Wyndham Worldwide Corporation’s board of directors stemming from three incidents between April 2008 and January 2010 in which personal credit card information of Wyndham’s customers was stolen by way of a cyber-attack on the company’s main network and those of its hotels.\textsuperscript{10} The Federal Trade Commission (FTC) initiated an investigation of the cyber-attack in April 2010, and in February 2014 a derivative suit was filed by shareholders. The shareholder derivative suit alleged that Wyndham “failed to implement adequate data-security mechanisms, such as firewalls and elaborate passwords, and that this failure allowed hackers to steal customers’ data.”\textsuperscript{11} While this case was ultimately dismissed without addressing the merits of the plaintiff’s claims, it serves as an important warning to directors that potential liability can result from data security breaches. Further, directors should take heed that commentators predict an increase in the number of suits against directors of companies that have a data security breach, alleging that the board failed to properly monitor the company’s data security efforts and ignored warnings which resulted in the security breach.\textsuperscript{12} In addition, boards will likely face claims that they failed to take appropriate action after a security breach to mitigate the damage from the breach.

\textit{Nonprofit Directors}

Nonprofit directors should closely monitor developments related to director liability for data breaches occurring in the for-profit arena. While it is true that some state statutes provide directors of nonprofit organizations with immunity from liability for civil damages resulting from acts or omissions relating to the director’s position as a director, such immunities generally do not apply to a director’s willful or grossly negligent acts or

\textsuperscript{10} Dennis Palkon et al. v. Stephen P. Holmes et al., Case no. 2:14-cv-01234.
\textsuperscript{11} Id.
\textsuperscript{12} John E. Clabby, Joseph W. Swanson, “A Firewall for the Boardroom: Best Practices to Insulate Directors and Officers From Derivative Lawsuits and Related Regulatory Actions Regarding Data Breaches,” Bloomberg BNA, available at \url{www.bna.com/firewall-boardroom-best-n17179935099/}. 
Therefore, if a court were to conclude that a board’s failure to oversee a nonprofit provider’s information security program was so inadequate that it amounted to gross negligence, the director could face liability despite statutory immunity.

It is also important to note that in states in which nonprofit directors do not have statutory immunity, they face liability for breaching their fiduciary duties. For example, in a recent case, *In re Lemington Home for the Aged*, the Third Circuit held the directors of a nonprofit nursing home liable for, among other things, breaching their duty of care for recklessly failing to remove the nursing home’s administrator and chief financial officer.  

In this case, evidence showed that the directors were aware that the home was mismanaged and had “three times the deficiencies of the average nursing home operating in the state,” yet they did nothing to remediate these problems. Such a case serves as a valuable reminder that even nonprofit boards may be liable for failure to “exercise reasonable diligence and prudence in their oversight” of the organization.

**Key Laws Relevant to Health Care Information Governance**

In order for a health care director to understand his or her proper role in overseeing cybersecurity, the director must first be aware that there are a plethora of laws and regulations governing the protection of confidential information in the health care arena. Three primary sources of legal requirements include: (1) the Health Insurance Portability and Accountability Act (HIPAA); (2) state breach notification laws; and (3) Section 5 of the Federal Trade Commission Act (FTCA).

**HIPAA**

HIPAA requires covered entities and their business associates to safeguard the confidentiality of their patients’ protected health information (PHI), including PHI that is

---

13 Id.
15 Id.
16 Id.
electronically maintained or transmitted by the covered entity or business associate.\textsuperscript{17} PHI is individually identifiable health information, which: (1) “[i]s created or received by a health care provider, health plan, employer, or health care clearinghouse”; (2) relates to the individual’s physical or mental health, the provision of health care to the individual, or payment for providing such health care; and (3) either identifies the individual or reasonably could be used to identify the individual.\textsuperscript{18}

HIPAA only applies to covered entities and business associates.\textsuperscript{19} Covered entities include health plans, health care clearinghouses, or any health care provider that transmits health information in electronic form in connection with transactions for which the Secretary of the Department of Health and Human Services (HHS) has adopted standards under HIPAA.\textsuperscript{20} Business associates are generally third-parties that create, receive, maintain, or transmit PHI on behalf of the covered entity, or that provide services to or for a covered entity (including legal, actuarial, accounting, consulting, data aggregation, management, administration, or financial services) that involve disclosure of PHI to the third-party.\textsuperscript{21}

HIPAA has three categories of regulations relevant to a discussion of cybersecurity issues: the Privacy Rule, which protects the confidentiality of PHI; the Security Rule, which sets standards for the security of electronic PHI; and the Breach Notification Rule, which requires covered entities and business associates to provide notifications to the government and affected individuals after certain breaches of PHI. The HHS Office for Civil Rights (OCR) oversees enforcement of HIPAA through the investigation of complaints and compliance reviews. HIPAA violations and settlements over alleged violations can lead to steep civil monetary penalties, as much as $50,000 per violation. For example, in May 2014 New York - Presbyterian Hospital (NYP) agreed to pay OCR $3.3 million to settle charges that it had potentially violated HIPAA after “a computer server that had access to NYP ePHI information systems was errantly reconfigured” and

\textsuperscript{17} See 45 C.F.R. § 164.302(2013).
\textsuperscript{18} See 45 C.F.R. § 160.103 (2013) (defining “protected health information and individually identifiable health information”).
\textsuperscript{19} See 45 C.F.R. § 164.302 (2013).
\textsuperscript{20} See 45 C.F.R. § 160.103 (2013) (defining “covered entity”).
an OCR finding that NYP had, among other things, failed to conduct an appropriate risk analysis under the Security Rule or implement appropriate security measures.\textsuperscript{22}

Numerous HIPAA violations and settlements have arisen in recent years, serving as a valuable reminder to health care boards of the importance of ensuring compliance with this law.\textsuperscript{23}

Although HIPAA requires covered entities and business associates to implement appropriate “Administrative,” “Physical,” and “Technical” “Safeguards” to protect the confidentiality of a patient’s PHI, it does not prescribe the exact measures that an entity should take to ensure the confidentiality of this information. Instead, each organization is required to examine its systems and resources and to develop appropriate safeguards to protect patients’ PHI.\textsuperscript{24} In addition to requirements imposed by HIPAA, health care entities must also comply with state privacy laws that often provide greater protections for PHI than HIPAA.\textsuperscript{25} Given the severe penalties that can result from violations of HIPAA and comparable state laws, directors must ensure that the providers they serve have a comprehensive plan in place to protect the confidentiality of their patients’ PHI from attack by cyber terrorists.\textsuperscript{26}

\textit{State Data Breach Notification Laws}

Forty-seven states, the District of Columbia, and Puerto Rico all require persons or organizations possessing personally identifiable information (PII) of their residents to

\begin{itemize}
\item \textsuperscript{22} U.S. Department of Health & Human Services Press Release, “Data Breach Results in $4.8 Million HIPAA Settlements” (May 7, 2014).
\item \textsuperscript{23} See, OCR’s Breach Portal, commonly referred to as the “Wall of Shame” available at https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.
\item \textsuperscript{24} For example, CMS explains that the HIPAA “Security Rule is based on the fundamental concepts of flexibility, scalability, and technology neutrality. Therefore, no specific requirements for types of technology to implement are identified.” HIPAA Security Series, Security Standards: Technical Safeguards Department of Health & Human Services, p. 4, available at www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf.
\item \textsuperscript{25} See 45 C.F.R. § 160.203 (2013).
\item \textsuperscript{26} In addition to HIPAA, health care entities must comply with numerous other laws and regulations requiring them to safeguard the privacy of a patient’s information, including the Federal Educational Rights and Privacy Act, Title X of the Public Health Service Act, and the Genetic Information Nondiscrimination Act.
\end{itemize}
notify the residents if their PII is compromised by a security breach.\textsuperscript{27} States commonly define PII as a combination of the resident’s name and other identification information such as a resident’s Social Security Number, driver’s or state identification number, or financial account or card numbers with account access information—such as security or access codes or PINs.\textsuperscript{28} Some states also include medical information in their definition of PII.\textsuperscript{29}

State breach notification laws generally apply to persons or entities that “own or license” PII. While not all states provide a definition for own or license, Missouri’s definition includes “personal information that a business retains as part of the internal customer account of the business or for the purpose of using the information in transactions with the person to whom the information relates.”\textsuperscript{30} Entities, including nonprofit entities, covered by state breach notification laws must provide timely notice to affected consumers of a known security breach. They may also be required to provide notice to consumer reporting agencies and state authorities depending on the number of consumers affected by the breach.\textsuperscript{31} If an entity has an effective method of encrypting electronic PII, such as symmetric and asymmetric methods, it is usually exempted from breach notification obligations.\textsuperscript{32} Entities that fail to comply with applicable breach notification laws face significant civil fines and court orders enjoining them from further violations.\textsuperscript{33}

A health care entity should be prepared to comply with state breach notification laws in the event its systems are compromised by a cyber-attack and PHI falls into the hands of cyber terrorists. Given the difference in state mandates and swift consumer notice requirements, directors must confirm that their organization have a crisis response plan

\textsuperscript{27} National Conference of State Legislators, State Breach Notification Laws,\textsuperscript{ available at www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.}

\textsuperscript{28} Id.

\textsuperscript{29} See, e.g., ARK. CODE. § 4-110-103, CAL. CIV. CODE § 1798.80. Also, Illinois has proposed legislation to include medical information, health insurance information and unique biometric data in the definition of “personal information.” 2015 IL S.B. 1833.

\textsuperscript{30} MO. REV. STAT. § 407.1500.1(7).

\textsuperscript{31} See, e.g., VA. CODE ANN. § 18.2-186.6(B), (E).


\textsuperscript{33} See, e.g., ME REV. STAT. TIT. 10, § 1349(2), CAL. CIV. CODE § 1798.84, IDAHO CODE ANN. § 28-51-107.
in place prior to any security breach to ensure that the entity is capable of complying with all applicable legal mandates.

**Section 5 of the FTCA**

In recent years the FTC has instituted multiple data security enforcement proceedings against health care entities for alleged violations of Section 5 of the FTCA.\(^{34}\) Section 5 of the FTCA prohibits “unfair or deceptive acts or practices in or affecting commerce.”\(^ {35}\) To pursue an entity for committing an “unfair” act under Section 5, the FTC must prove that the “act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.”\(^ {36}\) To prove deception, the other basis for a Section 5 claim, the FTC must establish that the entity committed a material misrepresentation, such as failing to comply with statements within its privacy policy, which results in harm to consumers.\(^ {37}\) The FTC imposes considerable penalties for violations of Section 5 by, among other things, levying fines and requiring the violator to file detailed reports with the FTC demonstrating how the entity is complying with applicable requirements.\(^ {38}\)

In various suits the FTC has asserted that Section 5 of the FTCA requires certain categories of personal information to be safeguarded by health care entities, including: patient names with billing information and diagnostic information, genetic information, medical histories, health care providers’ examination notes, and medical health history profiles. Such categories are comparable to PHI under HIPAA.\(^ {39}\) In addition, it is important to note that in August 2015 the Third Circuit unanimously concluded that the FTC has authority to regulate a company’s cybersecurity efforts. This decision stemmed

---


from the attacks on Wyndham discussed above. In this case, the court affirmatively concluded that Wyndham’s failure to maintain appropriate security measures could constitute an “unfair” practice under the FTCA.\textsuperscript{40} This decision, combined with the FTC’s position that Section 5 protects certain health information, puts directors in the health care industry on notice that if the provider’s IT system is compromised and patients’ medical information is disclosed, the provider faces a significant risk that the FTC will be able to prevail on a claim that the provider violated Section 5 of the FTCA resulting in significant penalties for the entity.

**Director’s Role in Cybersecurity**

While an organization’s executives and IT managers are responsible for the creation and implementation of the entity’s data security program, directors are responsible for overseeing these responsibilities and must exercise due care in discharging this duty. This requires directors to, among other things: (1) be cyber literate; (2) oversee the entity’s risk assessment of its information security practices; (3) ensure that appropriate resources are dedicated to cybersecurity; (4) consider obtaining cyber insurance; (5) oversee relationships with third-party service providers; (6) assign responsibility for cybersecurity oversight; and (7) ensure that the organization has a crisis management plan in place.

**Directors Must Be Cyber Literate**

A major barrier to a board’s effective oversight of cybersecurity is the lack of cyber literacy among directors. In spite of mounting risks posed by cybersecurity and countless examples of catastrophic data breaches, boards often struggle to understand IT security issues due to a lack of knowledge about, and experience in, this area. A recent National Association of Corporate Directors (NACD) study found that more than three-quarters of public company director respondents conceded that they personally

\textsuperscript{40} *Federal Trade Comm’n v. Wyndham Worldwide Corp., et al.*, No. 14-3514 (3d Cir. 2015).
could benefit from a greater understanding of IT issues, while almost 90% perceived that their board’s IT knowledge could be improved.\footnote{National Association of Corporate Directors, “Cyber-Risk Oversight,” Director’s Handbook Series (2014).} Boards can improve their understanding of cybersecurity by recruiting directors with IT experience such as chief information officers or individuals responsible for IT security efforts in organizations of a similar size with similar industries.

In addition to recruiting experienced directors, companies can help their directors become cyber literate by including IT topics as part of their regular board educational sessions. During these sessions, management and/or outside advisors should provide the board with essential information about the overall operation of the organization’s IT systems, the operation and validation of its IT security efforts, and best practices in the industry. Additionally, providers should consider having external advisors provide the board with an independent assessment of the adequacy of the organization’s information security efforts, including information on the entity’s ability to detect and respond to security breaches and how the organization’s information security program compares with that of other organizations of similar size and scope.\footnote{Id.}

\textit{Oversee Risk Assessment}

HIPAA and other legal mandates governing a health provider’s information security practices grant organizations considerable freedom to determine how to protect confidential information. This zone of discretion within the law makes the development and implementation of data security practices in health care organizations as much a strategic, risk-management decision as it is an exercise of legal compliance. Therefore, it is incumbent on directors to understand the organization’s approach to information security and the risks involved with the approach.

While there are many methodologies an organization can use to assess the risks posed by its information security systems, the HIPAA Security Rule provides one example of
an approach to this analysis. The HIPAA Security Rule requires organizations to conduct a seven-step process designed to assess a system’s ability to protect the confidentiality, integrity, and availability of PHI. These steps include an evaluation of the organization’s culture and commitment to data security, the development of an action plan to mitigate identified risks, and the monitoring and auditing of security on an ongoing basis. Expanding the HIPAA “risk analysis” approach beyond concerns regarding PHI can also serve as a method of assessing the organization’s ability to protect confidential information that may not be protected under HIPAA.

To fulfill their oversight duties, directors are not required to actually engage in their own analysis of the risks presented by the organization’s security efforts. Instead, directors must engage in a “process of asking the right questions of management to determine the adequacy and effectiveness of the organization’s [security] program, as well as the performance of those who develop and execute that program, and to make compliance a responsibility for all levels of management.” Further, directors must make sure that the risks presented by the entity’s security program, and the efforts taken to mitigate the risks, are appropriate in light of the economic and operational realities facing the organization. Because cyber threats are constantly evolving, to effectively discharge their oversight duties, directors must continuously engage in an active dialogue with management regarding the cybersecurity risks facing the organization.

Ensure that Appropriate Resources are Dedicated to Cybersecurity

As a vital component of risk management, directors must ensure that the health care entity has dedicated appropriate resources to its cybersecurity efforts. In an environment in which providers are facing reductions in reimbursements and other financial challenges, a board may have difficulty justifying significant expenditures on information technology and may actually see information technology as an area where

---

43 The Office of the National Coordinator for Health Information Technology, “Guide to Privacy and Security of Electronic Health Information” (April 2015).
44 Id.
expenses could be cut. In making these budgetary decisions, however, boards must be cognizant of the significant damages, both monetary and reputational, that can be inflicted on the organization from its failure to properly invest in IT systems. In addition to ensuring that appropriate financial resources are dedicated to protect against cyber-attacks, boards should also make sure that management has engaged individuals with the right expertise and experience to help guard against cyber-attacks. One way boards can exercise this oversight is by requesting regular reports directly from the Chief Information Officer (CIO) or other person in charge of IT. By receiving reports directly from the CIO, rather than indirectly from the Chief Executive Officer or Chief Financial Officer, not only will the board be able to directly assess the abilities of personnel responsible for IT security, but the board will also obtain direct insight into the provider’s cybersecurity efforts.

Consider Cyber Insurance

As part of its cyber-risk management strategy, a board should consider whether it is appropriate and cost effective to transfer some of the risk of cyber-attacks through insurance. While many directors may believe that the organization’s general commercial liability insurance policy covers cyber-attacks, it is important to note that in many instances these types of policies do not include coverage for cyber-attacks. Therefore, to effectively mitigate the risks associated with cyber-attacks, a provider may need a specific and distinct cyber insurance policy.

It should be noted that cyber insurance is often expensive and the coverages are often subject to dispute. For example, a New York federal court currently presides over a dispute between Federal Insurance Co. and Medidata Solutions Inc. regarding the scope of coverage provided by a cybersecurity policy. The dispute arose after a criminal persuaded an employee in Medidata’s finance department to transfer nearly $5

---

46 The New York Supreme Court held in *Zurich American Ins. Co. v. Sony Corp. of America, et al.* (N.Y. Sup. Ct. Feb 21, 2014) that the general liability insurance policy Sony maintained, which included coverage for “bodily injury” and “property damage,” did not cover damages resulting from cyber attacks.

million to a bank account in China in response to emails the individual thought came from a company executive.\footnote{Id.} The insurance company is attempting to avoid coverage by claiming that the policy only covers transfers effected by hackers and does not cover voluntary transfers by authorized persons.

When evaluating cyber insurance, directors should obtain advice from insurance brokers or other independent experts to make sure that the scope of coverage is appropriate and that the directors understand all applicable limits and exclusions. While cybersecurity insurance may not be appropriate for all providers, boards must at least examine the costs and coverages, given the potentially severe damage that can result from a major data breach.

Assigning Responsibility for Cybersecurity Oversight

No general consensus exists in health care or other industries regarding whether cyber risk oversight should be the responsibility of the entire board or confined to a board committee, such as the audit committee. According to a survey conducted by the NACD, 53% of directors believe risk oversight responsibilities should be assumed by the entire board.\footnote{National Association of Corporate Directors, “Cyber-Risk Oversight,” Director's Handbook Series (2014).} Similarly, the NACD Blue Ribbon Commission on Risk Governance advocates for risk oversight to be a function of the full board.\footnote{Id.} Yet despite such recommendations, a considerable number of boards allocate the responsibility of risk oversight to the audit committee.\footnote{Id.}

Given the intricate and constantly changing nature of cyber-threats, delegation of cyber-risk oversight to a particular committee may enable certain directors to devote the necessary time and effort to effectively oversee such risks. However, boards that allocate cyber-risk oversight to an audit, risk, or other committee must ensure that the

\footnote{Id.}
\footnote{Id.}
\footnote{Id.}
committee provides periodic briefings of its efforts to the entire board.\textsuperscript{52} In addition, cybersecurity issues should be considered by all directors when contemplating larger decisions such as IT system upgrades, mergers and acquisitions, or other major organizational decisions and all directors should understand how the risk of a cyber-attack can affect other risks, such as regulatory compliance risk.\textsuperscript{53} Regardless of whether responsibility is assigned to a committee or the entire board, boards must now prioritize cybersecurity and make oversight of cybersecurity a recurring agenda item.

\textit{Oversee Relationships with Third-Party Service Providers}

The potential for data breaches of PHI or PII caused by an organization’s third-party service providers present an additional vulnerability that directors must consider. In a study conducted by security firm, Trustwave, of 450 data breaches that occurred in 2013, almost two-thirds of the breaches were linked to third-party providers.\textsuperscript{54} Therefore, in addition to inquiring whether an organization has appropriate business associate agreements in place with all third-party providers that meet the definition of a business associate as required by HIPAA, directors should understand the entity’s standard contractual provisions with third parties. Specifically, directors should inquire whether these provisions require third parties to indemnify the provider from liabilities caused by breaches of the third party’s systems, to maintain appropriate insurance and to notify the provider in the event its systems are compromised. Notification requirements are especially important given the myriad of state data breach notification laws described above.

\textit{Ensure Hospital Organization has an Effective Crisis Management Plan in Place}

Because there is no guarantee against a cyber-attack, director oversight requires directors to ensure that management is appropriately prepared for a cyber-incident. This

\textsuperscript{52} Id.
\textsuperscript{53} Id.
\textsuperscript{54} Trustwave Global Security Report, 2013, Trustwave Holdings Inc.
requires the board to ensure that management has a crisis management plan in place and has rehearsed the plan. The plan should address, among other things, who would lead the investigation of a data breach and what steps would be taken to mitigate the damage from the breach and to begin remediation efforts, including notifying appropriate authorities, if necessary. The board may also want to consider whether the organization should have established engagements with key experts, such as law firms, to ensure that it is able to immediately and appropriately respond to a data breach.\textsuperscript{55} Failure to do so may lengthen the response time to a breach as well as increase the cost of securing such services.

Finally, a comprehensive disaster plan must contemplate how the organization as a whole would continue operations in light of a cyber-attack impacting the organization’s operational infrastructure, including the possibility of losing network connectivity or access to critical information.

Conclusion

Cybersecurity can seem daunting for directors considering the multitude of laws requiring providers to protect the confidentiality of their patients’ information and the significant damage a cyber-terrorist can inflict on an organization. It is, however, important for directors to understand that their responsibilities for oversight of a provider’s information security program are similar to their oversight responsibilities for other risks facing the organization. Directors must use their judgment and knowledge to provide effective guidance to management to ensure that the provider’s information security program is appropriately designed and operated given the business realities facing the organization.

*Kirstin Salzman, a partner in Husch Blackwell’s Healthcare, Life Sciences & Education practice, provides transactional legal guidance and strategic advice to a wide range of clients in health care and other industries. She counsels these clients in mergers,

\textsuperscript{55} \textit{Id.}
acquisitions, joint ventures, governance issues, private equity and venture capital investments, employment agreements, outsourcing transactions and other complex contractual arrangements. Her practice is national in scope, and she has represented Fortune 500 public companies, mid-sized and smaller private companies, and large nonprofit hospital systems. In addition, she regularly advises boards of trustees on governance issues.

David Solberg is a member of Husch Blackwell’s Healthcare, Life Sciences & Education group. David focuses his practice on serving health care and higher education institutions. He advises health systems and other covered entities on compliance with the Health Insurance Portability and Accountability Act, Emergency Medical Treatment & Labor Act, and provider licensure laws. David also provides counsel to higher education institutions regarding compliance with the Clery Act, Americans with Disabilities Act, Family Educational Rights and Privacy Act, Title IX, and the return of Title IV funds.