Cyber Risks: Board Responsibilities

Related Professionals

Anthony Spina

Related Services

Corporate and Business Organizations

Related Industries

Financial Institutions

AUTHORED ARTICLE | Summer 2014

The Bankers' Statement – Summer 2014

Published in the Summer 2014 issue of *The Bankers' Statement*

With developments over the recent years that include a number of high profile data breaches (e.g., Snowden and Target), the National Institute of Standards and Technology release of its recommendations titled the "Framework for Improving Critical Infrastructure Cybersecurity," and the enhanced regulatory exam focus on identifying an institution's preparation and protections related to cyber risks, institutions and boards that fail to focus and create plans to deal with cyber risks do so at their own peril.

Although most may conjure up thoughts of an internet hacker sitting at his computer attempting to access restricted information from a company's website when they hear the term "cyber risk," the term can and should be interpreted much more broadly. Institutions should consider both online risks (e.g., internet access to funds and data) and offline risks (e.g., tablets and smartphones containing protected data), and also realize that the exposures created could originate internally (e.g., employee) or externally (e.g., ex-employee, third-party vendor or stranger). In addition, the individuals creating the exposure may have a malicious intent (e.g., stealing consumer data to sell or the transfer of bank or customer funds) or simply have created the exposure accidentally (e.g., losing a tablet or smartphone containing accessible protected data).

Cyber risks are clearly a critical component of the board's responsibilities with regard to enterprise risk management. The potential for discovering that your institution's balance sheet has been compromised and assets have been stolen and moved offshore, that customer funds have been accessed, or that your institution has lost a significant amount of protected information through a data breach, should unfortunately keep directors up at night. The expenses that are generally associated with cyber risks are usually significant, and include costs related to lost customer and bank funds, card reissuance, account monitoring fees, fines imposed by credit card companies, class action lawsuits from customers, reimbursement to consumers for fraudulent

transactions, and shareholder liability for failing to prevent the data breach or properly disclosing the cyber risks. Not to mention the reputation risk and adverse impact on business resulting from such actions.

Directors, in their fiduciary role and under their important common law "duty of care," cannot ignore these risks and their responsibility to implement and oversee enforcement of appropriate and adequate controls to address and mitigate the potentially devastating impact of these issues.

While cyber risk may have originally been a large institution problem, it has also become a very real concern for smaller institutions as they continue to expand their cyber risk profile (and exposure) by increasing access to internet banking, customer processing terminals and providing other electronically based products and services. In addition, sophisticated cyber criminals, who may have previously limited themselves primarily to larger institutions, are increasingly targeting smaller institutions that they assume have less sophisticated controls in place to defend against their cyber attacks. The cyber risks not only have a potential direct financial impact on the institution, but also create significant reputational risk for the institution going forward as customers and the public learn of the exposure.

Based upon these potential threats, boards should actively inquire and receive ongoing assurances regarding how their institution is currently addressing its cyber risks, what controls are currently in place, who is monitoring those controls, and what steps are being taken in order to ensure that both the staff and other related parties are following appropriate procedures. Management and the institution's auditor must be prepared to respond with a specific, cogent and credible plan to any inquiries made by the institution's regulators and board. Directors who fail to address and document the efforts they have taken to protect their companies from cyber risks may well encounter regulatory criticism and potential regulatory and shareholder exposure should a successful cyber attack or breach occur.

Insurance and Indemnification

Along with evaluating and assessing the nature and extent of the institution's cyber risks and developing plans to deal with the potential exposures, directors should review relevant aspects of the institution's entire insurance program. The review should include not only an analysis of the institution's traditional insurance policies (i.e., commercial general liability insurance, commercial property insurance, crime policies and director and officer insurance), but should also consider the option of purchasing a specific Cybersecurity Liability Insurance Policy (Cyber Policy) to fill any gaps. Keep in mind that traditional insurance policies generally do not offer insurance protection for cyber risks and may contain specific exclusions. Each institution's policy may vary and the specific language of your insurance policies should be reviewed.

While Cyber Policies have not yet been standardized and the market for Cyber Policies is still in its infancy, directors should consider whether purchasing a Cyber Policy makes sense for the institution. Cyber Policies generally provide coverage that is not available under the institution's traditional insurance policies, but care should be taken to find someone with experience (i.e., insurance agent or attorney) that can assist with the review of the Cyber Policies being considered. In addition, because the products are not standardized it is easier to negotiate and tailor a product to your specific institution needs.

Insofar as the coverage afforded will vary by insurance company, Cyber Policies, generally speaking, can be negotiated to include:

1. liability expenses (i.e., defense costs, damages, loss of customer funds and regulatory fines) connected to network security failures, wrongful disclosure of information, regulatory investigations and violations committed by an outsourcer;
2. first party losses suffered by the institution and caused by a network related business interruption, system failure business interruption, intangible asset damage and reputation damage; and
3. expenses paid by the institution to a third party vendor in connection with an incident (i.e., crisis management, breach related legal advice, forensic investigation, call center, credit monitoring and cyber extortion payments). Keep in mind that not all coverages may be offered by all insurance companies.

Further, the board should review director indemnification provided by applicable law and by the institution's governance documents to ascertain that it provide appropriate protections for directors in the event that claims arise. The nature and amount of indemnification may vary, as does applicable D&O insurance coverage, and board may desire to ascertain that they have the most current and favorable indemnification coverage (and corresponding insurance to protect the institution) available for the type of risks involved.

Conclusions

Cyber-security and cyber-risk have become "hot buttons" in the financial services industry, and a very important part of the board's risk-management responsibilities. Institutions should expect a significant focus on cyber-risk in upcoming examinations, and even perhaps off-schedule intervening visits and questions by regulators regarding the institutions cyber security programs. As a very real risk exposure in the industry, directors should be taking additional precautions to assess institutional cyber risk, to ascertain that their institutions are adequately prepared to address cyber risk issues and exposures, and to ascertain that appropriate insurance and indemnification protections are in place to protect the institution and its board.

Please contact your Vorys attorney should you need assistance regarding the board's duties and obligations with respect to cybersecurity and other matters, or to discuss and review cybersecurity insurance policies and other related protections for the board and the institution.