WINTER 2014
www.bdo.com

AN OFFERING FROM BDO'S CORPORATE GOVERNANCE PRACTICE

BDO BOARD REFLECTIONS

CYBERSECURITY – A Board Primer

Whether it be the media focus on the numerous cyber breaches reported at businesses of all sizes, demands from the public and shareholders to safeguard cyber assets, scrutiny from government agencies or simply the daily reminders to individuals as their identities and personal information fall victim to online predators, more and more board agendas are targeting cybersecurity as a primary risk management area for their companies. However, there still seems to be a lack of understanding by boards in terms of what cybersecurity encompasses, what role the board may play in the process and how to best protect organizations against cyber breaches.

Safeguarding of an organization's assets extends to cyber assets. Cyber assets comprise programmable electronic devices and communication networks including hardware, software and data. The use of such assets is becoming more prevalent, expanding the capabilities and speed in which business is transacted and communications are made. Keeping up with the pace of development and globalization of cyber assets is proving challenging.

What are cyber breaches and how do they occur?

A cyber breach is an unauthorized access to and/or dissemination of electronic information. It may be due to an attack on a data network or outright theft of documents, portable devices, USB drives, laptops, etc. Breaches ensue when hackers and others exploit weaknesses in lacking or faulty protections around cyber data.

Whether cyber attackers act on the information they access or not, the mere fact that individuals without authorization to access such information can obtain it is a cyber breach. The abilities of

▶ Read more

BDO USA CORPORATE GOVERNANCE PRACTICE

BDO USA's Corporate Governance Practice was developed to provide guidance to corporate boards. The firm works with a wide variety of clients, ranging from entrepreneurial businesses to multinational Fortune 500 corporations, on a myriad of accounting, tax, risk management and forensic investigation issues.

CONTACT

For further information about cybersecurity, please contact:

MICHAEL BARBA
212-885-8120 / mbarba@bdo.com

LEE GRAUL
312-616-4667 / lgraul@bdo.com

JEFFREY HALL
212-885-7339 / jhall@bdo.com

DEAN IRWIN
214-665-0606 / dirwin@bdo.com

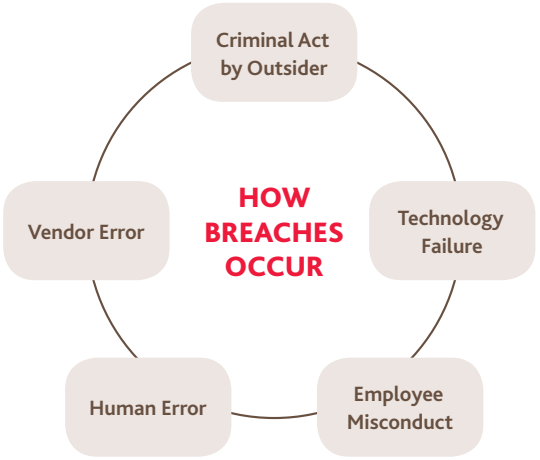
AMY ROJIK
617-239-7005 / arojik@bdo.com

USE OF SOCIAL MEDIA

Use of social media is an evolving area for companies and is beginning to extend beyond advertising, recruiting and employee retention to voluntary disclosure of financial and other sensitive information to investors and potential investors. In April 2013, the SEC issued a report making it clear that companies can opt to use social media outlets like Facebook and Twitter to announce key information in compliance with the Regulation Fair Disclosure (Regulation FD) so long as investors have been alerted about which social media will be used to disseminate such information. A key task for management as well as boards will be to be diligent in following proper disclosure practices and educating their employees to do the same. But how quickly is the use of social media as a disclosure vehicle catching on? In a recent BDO USA, LLP Board Survey, board members of mid-market public companies indicated that while they were aware of the ability to disclose information via social media, only 11 percent anticipate utilizing social media for material disclosures in the future.

those with malicious intent seem to know no bounds and that alone should be a critical concern of everyone that utilizes any form of electronic data, particularly those charged with the safekeeping of corporate assets.

Are boards equipped to address cybersecurity risks?



The Carnegie Mellon Cylab Security Report of 2012 (Cylab Report) studied how a sample of board members and senior management from the Forbes list of global 2,000 companies were governing the security of their organizations' information, applications and networks (digital assets). The findings of the study were relevant then and remain so as the occurrence of cyber breaches continues to rise. In terms of bridging the gap between information technology risks and enterprise risk management, the report indicated "… boards are still not undertaking key oversight activities, related to cyber risks such as reviewing budgets, security program assessments and top-level policies; assigning roles and responsibilities for privacy and security; and receiving regular reports on breaches and IT risks." The result leaves companies potentially exposed to financial and reputational damage caused by theft and misuse of confidential and proprietary information.

Positive trends highlighted by the Cylab Report included a rise in the number of companies with designated board Risk Committees and cross-organizational teams to manage privacy and security matters along with more emphasis being placed on information technology (IT) and security and risk expertise in board recruitment. However, many companies still leave such vast risk responsibilities solely to the Audit Committee, whose segregation of duties may be compromised in that it likely oversees both the development of security programs along with the audits of controls and effectiveness of such programs. Furthermore, the Cylab Report cites that less than half the companies surveyed do not utilize external expertise to assist with cyber risk management.

What say the regulators?

In the public sector, the U.S. government is increasing congressional focus on U.S. Securities and Exchange Commission (SEC) action regarding adequacy of cybersecurity disclosures under the concepts that cyber attacks represent major economic and national security risks, and cybersecurity risks are as important to disclose as financial and operational risks. Citing inconsistencies and insufficiencies in current cyber risk disclosures, in April 2013, West Virginia Democratic Senator Jay Rockefeller specifically requested SEC Chair Mary Jo White elevate the SEC's Division of Corporation Finance's current Cybersecurity Disclosure Guidance to formal commission level guidance. In turn, Chair White has requested the SEC staff brief her on current disclosure practices and provide any recommendations it has regarding further action in this area, leaving the door open to additional action steps by the SEC.

Board's roles in guarding against cyber breaches

Boards are continually working to understand and fulfill their responsibilities related to guarding against cyber breaches. Reuters, via its Financial Regulatory Forum, posted a three part blog series on "Cybersecurity and The Board of Directors: Avoiding Personal Liability" which is quite informative and explores such questions, concluding that cybersecurity belongs on every board's agenda.

Reuters calls for boards to "require a comprehensive review of their organization's insurance policies to determine whether, and to what extent, they have coverage in the event of a cyber attack or breach." Cybersecurity insurance is designed to mitigate losses from a variety of cyber incidents, including data breaches, network damage and cyber extortion. The U.S. Department of Homeland Security (DHS) website describes cybersecurity insurance as an "effective, market-driven way of increasing cybersecurity because it may help reduce the number of successful cyber attacks by promoting widespread adoption of preventative measures; encouraging the implementation of best

▶ Read more

practices by basing premiums on an insured's level of self-protection; and limiting the level of losses that companies face following a cyber attack." DHS further indicates, however, that "…many companies nevertheless forego cybersecurity insurance altogether. They cite its perceived high cost, a lack of awareness about what it covers and uncertainty that they'll suffer a cyber attack as just some reasons for their decision."

A comprehensive cyber insurance plan includes coverage for both internal and external losses to the organization. Reuters categorizes internal losses as inclusive of business interruption expenses, legal expenses, loss of digital assets and security event response costs. External losses include third-party damages, credit-monitoring expenses, postage, advertising and customer notification, among other costs.

Differentiating between management and board roles in cyber risk management

Based on anecdotal observations, the following provides examples of how boards and management are differentiating their roles with respect to cyber risk management:

ROLE OF MANAGEMENT	ROLE OF BOARDS
Identify dedicated resources to address cybersecurity (e.g., CSIO)	Oversee organizational risk management
Assess risk and design and implement controls to protect the organization from breaches (internally/externally)	Understand and prioritize the risk of cybersecurity to the organization
Create a plan for addressing breaches – revisit plan periodically	Review processes, procedures, controls and education of employees designed by management and IT
Engage expertise prior to occurrence of a breach	Review plan for responding to cybersecurity breaches – revisit often
Develop and deliver continuous education to employees	Be informed of reported incidents – monitor
Liaise with internal auditors/external auditors to address adequacy of controls	Continue to receive education on cyber risks
Monitor and respond to reported incidents	

What are boards doing?

The following example reflects BDO USA, LLP's experience in working with our client boards as well as echoes many of the ideas expressed in some of the resources referenced within this practice aid to help boards define and develop a plan of action aimed at the protection of corporate cyber assets and the prevention of cyber breaches. Steps boards may consider in building an effective plan include:

- Create the appropriate organizational structure for managing cyber risk:
  - At the board level – Establish a dedicated Board Risk Committee – separate from the Audit Committee – with applicable risk experience along with the authority to enlist external expertise, as necessary
  - At the C-suite level – Establish a Chief Information Security Officer (CISO) position that reports to directly to the board[1]
  - At the Operational level – Establish a cross-functional team that meets regularly to review privacy and security issues and communicates up to the Risk Committee and CISO/CIO – include representatives from operations, human resources, legal, public relations, etc. and establish a subset of this team to serve as a "crisis response team" responsible for cyber breaches if and when they occur
- Set the tone for oversight of cyber risk management:
  - Make cyber risk management a critical board agenda topic and allocate appropriate time for identification and discussion of such risks – includes performing a risk assessment of known and potential cyber threats both internal and external to the organization
  - Review annually (or more frequently, as necessary) cyber risk policies, procedures and controls along with budgets for such established by management
  - Review privacy and security crisis management plans – which includes assessment of adequacy of breach notifications, cyber insurance coverage, public relations and communication plans, as well as addresses compliance complexities posed by varying state data breach notification statutes[2] and industry-sector regulations[3]
  - Request from the CISO regular metrics on cyber attacks, their source and method of mitigation and review incident reports of cyber breaches – Reports would clearly document what happened, how it happened, the extent of the damage and action steps to prevent recurrence
  - Establish systems to monitor cyber security infrastructure

1 Note: A CISO is distinguished from a Chief Information Officer (CIO) in that the CIO would be responsible for the design and implementation of the organization's data systems while the CISO would be responsible for testing security, conducting audits, and reporting on security weaknesses involving such data systems. To ensure proper segregation of duties, the CISO would report to the board or board committee much the same as the internal audit function would report to the audit committee.

2 Note: As of January 2014, 46 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have notification requirements for breaches of "personal information." Alabama, Kentucky, New Mexico and South Dakota do not currently have such data breach notification laws. For more information refer to: http://about.bloomberglaw.com/practitioner-contributions/complicated-compliance-state-data-breach-notification-laws/

3 For example, the HITECH Act which amends HIPPA for healthcare organizations; the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice pursuant to the Gramm-Leach-Biley Act (GLBA) for financial institutions; and the Federal Information Security Management Act (FISMA) for U.S. federal government agencies.

▶ Read more

  - Communicate to the entire organization, perhaps inclusive of vendors and other third parties, a no tolerance policy for cyber breaches
- Review annual audits of security programs conducted by competent professionals independent of management and assess whether any weaknesses identified are addressed on a timely basis
- Monitor delivery of continual education regarding cyber risk management for board members, management, employees, vendors and shareholders – includes keeping up to date on developments of new threats and new legislation/regulation
- Continue to ask questions such as:
  - Are we confident in management's risk management plans?
  - Are we allocating enough time and resources to cyber risk threats?
  - Do we have the proper expertise in house to advise us? Do we need to look externally?
  - Are we adequately insured as an organization against cyber breaches?
  - Where might weaknesses remain in our corporate infrastructure?
  - Do our remediation plans in the event of cyber breach go far enough to protect our assets as well as our organization's reputation and our customer relationships?
  - How might our business be impacted by a cyber breach? (Imagine worst case scenarios and plan accordingly!)
  - Are we receiving timely information from our CISO? Have all areas of the organization been considered in such assessments?
  - Is our organization's infrastructure keeping pace with increasing threats?
  - Are our public disclosures/communications adequate to instill public confidence in the measures we are taking to protect our investors' assets?
  - Are we doing enough to educate ourselves about cyber risk?

Key takeaways for consideration in managing risk in cyberspace

Technology continues to evolve at a record pace and the occurrence and cost of cyber breaches are rising at an alarming rate. More and more boards are making cybersecurity a risk assessment and risk management priority at their organizations. In this regard, organizations are striving to clearly define the roles and responsibilities of both management and the board. The deliverable for the organization then becomes an executable cybersecurity plan overseen by the board that is put into place by management in advance of a cyber breach. The periodic review of this plan by all parties to assess whether it is operating in line with assessed risk as well as the continual education at all levels within the organization is imperative to the successful management of cyber risk.

There is no such thing as completely secure data. Breaches can and do happen even in the most secure environments. This makes having a ready-to-implement incident response plan overseen by an engaged board even more critical.

For more information, access BDO USA, LLP's (BDO) and Latham & Watkins LLP's archived webinar "Managing Risk In Cyberspace" and the pending complement to this publication: BDO USA, LLP's "Responding to a Cyber Breach – A Board Primer."

Additional Resources

The following are links to additional resources boards may want to consider in assessing their organization's current cybersecurity plans:

- Carnegie Mellon Cylab Security Report of 2012
- Bloomberg Law Article "Cyber Risk and The Board of Directors – Closing the Gap"
- National Association of Corporate Directors (NACD) BoardVision: IT and Cybersecurity Video
- National Association of Corporate Directors (NACD) BoardVision: Privacy and Cybersecurity Video
- NACD Cybersecurity: Improvements Needed in the Boardroom
- Reuters Three Part Series: "Cybersecurity and The Board of Directors: Avoiding Personal Liability"
- Bloomberg Law Article "Complicated Compliance: State Data Breach Notification Laws"
- "Incident Response and Computer Forensics" by Chris Prosise, Kevin Mandia, Matt Pepe (for purchase)

▶ Read more