Breaching the silence on cyber security

For all the sound and fury, many boards spend surprisingly little time on cyber security. Here are 10 questions directors should be asking management.

By David Boehmer and Krishnan Rajagopalan

For boards of directors, cyber security is no longer an IT issue but an urgent matter of risk management. The list of risks is long and getting longer: theft of intellectual property, breaches of customer information, denial of service, malicious code, viruses, disclosures of information by disgruntled employees, and more. Meanwhile, yesterday’s cyber vandals have been joined by a new generation of online über-criminals, by other groups working closely with governments intent on stealing trade secrets and passing them on to their nation’s critical industries, and by “hactivists” with a political axe to grind. In October 2011 the SEC issued guidance to the effect that cyber attacks should be disclosed if they had material impact on a company’s operations or finances or were among the factors that could make an investment risky. In February 2013, an executive order and accompanying presidential policy directive instructed government agencies to work on cyber security issues with private owners of critical infrastructure in the U.S.

Yet for all the sound and fury, many boards spend surprisingly little time on cyber security. According to the Carnegie Mellon Governance of Enterprise Security: CyLab 2012 Report, a survey of senior executives and corporate board members from the Forbes Global 2000 list, “only about one-third of the boards that are engaged with privacy and security issues are focusing on activities that would help protect against reputational or financial losses flowing from data breaches and theft of confidential and proprietary information.”

To some degree, the silence in boardrooms is understandable. Cyber security is a technically complex subject; the IT structure is largely opaque to most directors, and many board members judiciously refrain from speaking up on matters they don’t understand. But the issue is much more than an IT one — cyber security extends across nearly every action a firm takes.

The ‘ask’ list

With so much at stake, boards should make sure that the management team is adequately addressing cyber risks, taking steps to mitigate them, and doing so within acceptable boundaries of risk tolerance. Directors can break the silence by asking these 10 initial questions:

• *Are we a likely target for cyber attacks?* Why and by whom? For any major, publicly traded corporation, the answer is almost always yes. Banks, credit card companies, transaction processors, and retailers are obvious targets, and they know it — many of the companies who disclosed their vulnerability to cyber attack on their 10Ks in 2012 were leading financial services institutions. Major defense contractors know it, too, and they have been testing a model with the U.S. government for national defense against cyber attack. Utilities, telecom companies, and other operators of critical infrastructure make rich targets for cyber warriors.

**David Boehmer** is the regional managing partner of the Americas for Heidrick & Struggles’ Financial Services Practice. His broad range of expertise spans across the banking, investment management, insurance, payments and transaction services sectors for roles including nonexecutive director, CEO, CIO, COO, and general management. **Krishnan Rajagopalan** is the global managing partner of the Technology and Services Practice. He focuses on leading senior-level searches for clients in the management consulting, technology services, outsourcing and venture capital arenas. He also conducts search assignments for executives in a broad range of corporate functions, including nonexecutive director, CEO, COO and president positions.
and companies in other advanced industries are obvious targets, but other targets might not be quite so obvious. With the rise of electronic health records, for example, healthcare organizations must protect sensitive data increasingly demanded by providers, payers, and employers and increasingly sought by cyber criminals for a variety of nefarious purposes. But even if your company’s exposure seems obvious, a forthright acknowledgement of that fact is a good way to begin the discussion.

• How many cyber breaches or incidents have we experienced, in what categories, and of what magnitude? According to the Economist, an annual study of 56 large American firms found that between them they suffered 102 successful cyber attacks a week in 2012, a 42% increase from 2011. Not all attacks are equal, of course. A theft of the credit card information for hundreds of thousands of your customers is far more serious than a prank designed merely to mock or embarrass the company. Further, a one-time breach differs from under-the-radar, sustained breaches that go on undetected, siphoning off valuable assets and information for extended periods of time.

• Who in the organization is chiefly responsible for cyber security? According to the Carnegie Mellon report, less than two-thirds of the respondents’ organizations have full-time personnel in key roles for privacy and security (CISO/CSO, CPO, CRO) in a manner that is consistent with internationally accepted best practices and standards. In many companies, responsibility is parcelled among a number of areas, often operating in silos: information security, data privacy, compliance, and risk management.

At the very least, the leaders in these areas should be working together. Ideally, however, the organization will have a CISO/CSO and a CPO, both of whom regularly present to the full board or the board risk committee. The top security officer should know technology, maintain good working relationships with law enforcement organizations and international agencies, and have the business acumen to grasp commercial risk. The CPO should have a similar grasp of technology and business issues and, especially, an understanding of reputational risk.

• What are our most valuable assets and what are we doing to protect them? Whether it is customer records, intellectual property, proprietary software. And once the firewall has been breached, how easy is it for attackers to move around inside your system? Ask also about proactive mechanisms the company uses to prevent intrusions and to respond to them once they are under way. You are not looking for a technical answer, but assurances that these steps have been taken and those mechanisms are in place.

• What are we doing about internal threats to cyber security? While the high-profile cases of Edward Snowden and Bradley Manning vividly illustrate the threat of bad actors operating on the inside, most companies confront a more prosaic but more pervasive internal security problem — unintended slip-ups or sloppiness on the part of employees. And for global companies, with thousands of employees and operations in many countries, the odds are high that someone somewhere will make a costly mistake.

According to IBM, 81% of employees use unauthorized devices like their tablets and personal smartphones on their company’s networks. Verizon reported earlier this year that three-fourths of network breaches were the result of weak or stolen usernames and passwords. Meanwhile, IT managers are expected to make sensitive company data accessible to more and more employees across all kinds of platforms and devices, many of which aren’t controlled by the company. Are policies, procedures, and incentives in place to make sure employees maintain vigilance in a highly porous cyber environment?

Regularly addressing cyber security ensures that the board is fulfilling its obligation to protect the enterprise.

— David Boehmer

pricing information, or systems that enable the company to transact business with customers, the company should have identified assets that are subject to cyber attack and assigned values to them. It should also be clear where those assets reside. Are they behind the firewall? In interfaces with business partners? In the cloud?

Protecting assets is more than a matter of a thick firewall and antivirus software. And once the firewall has been breached, how easy is it for attackers to move around inside your system? Ask also about proactive mechanisms the company uses to prevent intrusions and to respond to them once they are under way. You are not looking for a technical answer, but assurances that these steps have been taken and those mechanisms are in place.

• What do we do to make sure that we are considered a “trusted company”? Companies that forfeit the trust of their customers or business partners are asking for trouble. Creating trust starts at the top, with governance and company policies that convey the message that customer privacy and the safety of business partners’ intellectual property are paramount. What are the company’s relevant policies, how are they conveyed through the company, and what kind of accountability is in place?
• What is our budget for cyber security and how is it determined? Resources devoted to cyber security are often buried in IT budgets, which can obscure whether threats and risks are being adequately addressed. Ask management if these costs are being broken out separately to ensure that the organization is devoting sufficient resources to protecting its assets. Are threat levels and risks monitored, measured, and regularly reassessed to facilitate budget allocations? Further, the board should ask if the organization has adequate cyber insurance coverage — the most neglected aspect of cyber security, according to the Carnegie Mellon report.

• How much risk are we comfortable with? What is the level of cyber risk tolerance required to both protect the company and enable it to do business? Generally, of course, boards and management should be aligned about their tolerance for various kinds of risk: strategic, operational, compliance, reputational, and financial. Depending on the company and the industry, cyber security will impinge on each of those areas to differing degrees. Companies in consumer-facing industries face a great degree of reputational risk around customer privacy. High-tech and advanced industrial companies face strategic and financial risk around IP theft. And companies that represent critical infrastructure rightly worry about operational risk.

It’s tempting to say that when it comes to certain risks you will have zero tolerance, but it’s neither realistic nor financially feasible. Ask management to clarify the degree of risk current cyber practices entail in each area and make sure the board and management are aligned.

• Do we have a game plan in the event of a serious cyber breach? A comprehensive plan would include crisis management, business continuity and recovery planning, and clear roles and responsibilities for directors where appropriate. Is management prepared to act immediately? What is the policy about notifying law enforcement? Customers? The public? Companies have no choice — they must have a plan in place.

• What’s the plan to regularly update the board on cyber security? Once the board has recognized the magnitude of cyber issues, it should request regular updates from management, agree on the timing of the updates, and determine what they should cover. In a time when cyber attacks are becoming routine, regularly addressing them at the board level ensures that the board is fulfilling its obligation to protect the enterprise.

One final question to ask

Finally, there is an additional question that the board should ask: Do we have sufficient expertise among ourselves to exercise oversight of cyber risk? If not, it might be desirable to include such expertise in the profile for the next board appointment. That doesn’t necessarily mean adding a CIO or other technology expert to the mix, but it does mean finding someone who has knowledgeably and successfully exercised wise business judgment in the face of online enemies who are legion, invisible, and everywhere.

The board needs to determine whether ‘we have sufficient expertise among ourselves to exercise oversight of cyber risk?’

— Krishnan Rajagopalan

The authors can be contacted at dboehmer@heidrick.com and krajagopalan@heidrick.com.

Subscribe to Directors & Boards!

Directors & Boards is the thought leader in corporate governance, written by and for board members.

Individual subscriptions: $325 annually • Full board subscriptions: $2500 annually

Subscribe by phone at (800)637-4464, ext. 6072 or online at www.directorsandboards.com