Is It Time For A Board Cyber-Security Committee?

by Betsy Atkins

The past year saw names like Sony, Target and Home Depot grab headlines not for their business successes, but for their failures to cope with crippling cyber attacks. Does your board realize the vulnerability corporations today face from sophisticated hacking, and the massive potential damages? Is it time for boards to restructure themselves to better combat this threat?

In December, Sony Pictures revealed that it has been the victim of a massive cyber attack, with sophisticated hackers raiding the company networks for coming movies, corporate financial and salary records, and personal information about major stars (Sylvester Stallone even found his Social Security number leaked worldwide.)

In an article for the BBC's *Capital* blog, British corporate consulting expert Lucy Marcus went to the heart of the governance implications. "At every board meeting this month someone is bound to ask, either during the meeting or in a quiet aside, 'Could we be the next Sony?'" The saddest aspect of this is that corporate boards of companies around the world have already been asking much the same question for the past several years, only changing the name of the victim.

With so many data hacks sharing the same strategy, is something fundamentally broken in enterprise security that management and board oversight is unable to prevent?

Just the past 12 months have seen one massive corporate security breach after another. Major retailers (Target, Home Depot), e-commerce sites (eBay), and financial institutions (JPMorgan Chase) have all been victims. While the trend of breach after breach is unsettling, the far more important fact is that all of these attacks share the same multi-step blueprint for the attack.

In each case, the attack began by compromising one person with credentialed access—typically a partner or an employee. Then, that access was used to create an infected node that could burrow deeper into the network. This would then steal data stored internally, or infect additional systems that capture the target data, such as point-of-sale terminals. While it is still too early to tell how the massive Sony Pictures hack was organized, it likely used the same essential outline.

Taken individually, digital security breaches serve as a warning for executives and security professionals to remain vigilant. However, when every major breach shares the same telltale strategy, it is a sign that there is something more fundamentally broken in enterprise security that must be addressed.

Here is some of the damage that management and corporate governance oversight systems were unable to prevent:

- *eBay—145 million records compromised.* Multiple employee login credentials were accessed, and used to dig deeper into the network, and ultimately steal customer data.
- *JPMorgan Chase—76 million records compromised.* Access was gained through an employee laptop, and then spread across the network to find customer contact information.
- *Target—70 million records accessed.* Network was initially compromised via a partner (using their HVAC vendor's credentials). This then spread through the network, and pushed malware to the

Betsy Atkins *is founder of venture capital firm Baja LCC, and former CEO and chairman of Clear Standards, Inc. Her current board memberships include Polycom, Inc., HD Supply, Darden Restaurants, and Schneider Electric, SA. [betsyatkins.wix.com/betsyatkins]*

Target point-of-sale systems.

▫ *Home Depot—56 million records compromised.* Network was breached via a partner's credentials, and malware delivered to point-of-sale systems. The malware was a variant of the malware used at Target.

▫ *Michaels stores—Three million records compromised.* Michaels has not confirmed the details of how they were breached, only that there was a network breach, and affected terminals were all compromised with previously unknown malware.

▫ *Neiman Marcus—One million records compromised.* Network hacked and malware pushed down to the point-of-sale systems.

There are several important similarities in these attacks, all suggesting that your company data security protections need stronger oversight:

☐ ***Security looks for the first step, but misses the lifecycle of an attack.***

Traditional online security structures attempt to detect and block malicious payloads (either a piece of malware or vulnerability exploit). In the past, this was a very sensible approach, because the initial payload and the attack were one in the same. A basic programming query was fired at a vulnerable website, and the attacker gained a list of usernames and passwords. Malware was installed on a victim, and the hackers quickly spammed her contact list, and that was the end of the episode.

In a modern attack, the initial compromise is just a means to a much larger end. The first compromise provides the beachhead for the larger attack, which will be driven by a criminal who has done his homework on your organization. This can then play out over weeks, months, even years. The vast majority of security technologies are not designed to see the so-called "long con" of an attack.

Even though the security industry continues to develop more and more advanced methods of detecting individual pieces of malware, there is still too little ability to see the larger attack that follows after the malware. The attackers are playing chess, while your information security protections are still playing checkers.

☐ ***There are infinite opportunities for security systems to fail.***

As computing and business has evolved, the "attackable" areas of the enterprise have become nearly impossible to secure. Employees use mobile devices that are routinely outside the corporate firewalls. Corporate applications and data are increasingly both inside and outside the perimeter. Partners and customers need access to corporate applications and data in order to be competitive and efficient. Also, of course, attackers are constantly cooking up new attacks and strategies to evade detection.

All of this adds up to a near infinite number of chances for attackers to get the initial exploit of an attack past security. This then enables the internal phase of the targeted attack, beyond the protection of outward-facing firewalls, intrusion prevention systems, and malware sandboxes. Those who design prisons dedicate at most a few weeks or months to making them escape-proof. Those jailed in them, however, may have a life sentence of time to devise workarounds.

Here is a hard truth I have learned about corporate boards—directors really do not understand company security issues.

☐ ***Smart hackers will use your own security protocols against you.***

While security products can generate tons of data, it is often difficult to see the forest for the trees. For example, Target had indications that a new piece of malware was found in their network, but the context of the larger attack remained unclear. The Neiman Marcus breach generated thousands of low-priority informational alerts that were seen as false positives by the security team because the suspicious files looked like approved files that were allowed to be on the system.

In these cases and many others, it is obvious that data is not the same as insight. Security teams are often placed in the untenable position of trying to piece together conclusions from large amounts of data. Such a large amount of data is sometimes beyond the scope of what security was designed to detect.

Here is a hard truth I have learned about corporate

boards—directors really do not understand company security issues. In fact, most top corporate managers do not either. They fail to see all the resources that they must protect, what needs protecting, and just how vulnerable they actually are. This gap is even greater when it comes to the digital assets of the modern corporation.

Step one for every board is to understand that it is supposed to be offering oversight on these potentially devastating cyber-risks as part of its fiduciary duty.

There is no denying that it is difficult for directors to provide the oversight needed in this digital era. Online security has become incredibly complicated, and corporate directors may not even know the fundamental distinctions between the various types and motivations of online intrusions. For example, a basic hack may just be trying to steal credit card info, the digital equivalent of a "smash and grab" theft.

A higher-level, sophisticated cyber thief, on the other hand, may be targeting a particularly high-value corporate asset. This could be a seismic analysis of your oil/gas field, or a compound your pharmaceutical company has been working on for years. There may be cyber intrusions with national security or political aims, an attempt by foreign powers to access defense information or technology in your system, or an international hack to embarrass your company (as may have been the case with Sony America).

Your board likely lacks the expertise and oversight system to know the difference between a casual and a deep cyber threat, or know when data lost is something valuable—versus a breach that could completely put you out of business.

Step one for every board is to understand is that it is supposed to be offering oversight on these risks as part of its fiduciary duty. Your audit committee knows that it needs internal controls, like those mandated by Sarbanes-Oxley Section 404, to protect corporate assets. Likewise, the board now needs to assure internal controls to protect the corporation's cyber assets.

Shaping Your Cyber Board

Board Action Items For Cyber Security

- ☐ Management needs to encourage the board to fully embrace cyber security as a governance oversight responsibility. The board requires information and training on cyber security issues so they are not seen as too complex and technical, outstripping the board's ability to exercise oversight. Cyber security is not the exclusive province of the CIO. The board needs to know why and how it is expected to add oversight, and what that oversight might include.
- ☐ The board should consider whether a change needs to be made in the way cyber security oversight is currently handled at the board level. Is there a need for a new security compliance committee?
- ☐ The board may require new candidates with computer security background in the director nomination process. Would the "cyber savvy" of current directors give investors confidence?
- ☐ Given the risk exposure involved, the board should work with the general counsel to determine the extent to which existing D&O insurance coverage provides protection. Will you be protected if data breach-based legal actions assert personal liability against board members?
- ☐ For the board to exercise effective oversight, they will need an understanding of what matters are properly reserved for the CIO, what matters require board awareness, and what matters require board or committee oversight, action, and/or approval.

The stakes are high. In today's financial control environment, the chance of someone embezzling a large sum from the company through financial wrongdoing is fairly small. Yes, it happens, but it has grown far more difficult to successfully pull off such a scam. However, the amount of assets stolen and compromised through cyber-breaches is astronomical in comparison. A study found that up to $21 trillion in global assets could be at risk from cybercrime.

What is needed is a solid board structure for monitoring and managing cyber risk in the company. Oversight of cyber-risk at the board level is part of a larger mandate boards have faced over the past

decade—that of properly managing risk overall. The economic crisis of 2008-2009 found many boards caught unaware of the financial and market risks their companies were exposed to, and board oversight structures have spent the past few years rushing to catch up.

Audit committees were seen as the most natural slot for the risk oversight portfolio. The committee performs a wide range of oversight responsibilities, from financial controls and compliance to other corporate risks. However, I believe there is a big gap in most audit committees when it comes to understanding the unique cyber-security vulnerability of companies. Audit, by definition, deals in financial figures, and issues that do not lend themselves to a spreadsheet can be difficult for them to oversee.

If your board chooses to make its audit committee the home of cyber-security oversight, start by upgrading its capabilities. Audit committees need to better understand how security threats strike so they can provide better oversight and risk management. The first step I recommend is a series of committee briefings so "cyber security" is demystified and better understood. The company's objectives to protect critical information, client identities, and financial vulnerability should be discussed. I also recommend requesting a security plan that can be audited.

However, given the complexity and dangers involved, I think the time has come for boards to create a dedicated cyber-security technology committee. Boards currently have three standard standing committees (audit, compensation, governance/nominating). Depending on the industry, they may then add specific additional committees. For example, manufacturing company boards often have an OSHA safety committee. Chemical, oil and gas companies may have an environmental committee. Clearly, any corporation that faces the consumer, such as retail, financial services, or consumer packaged goods, ought to have a standing security and tech committee.

How to go about setting up this new board committee?

☐ *Identify the knowledge and background this committee needs, and recruit new board members with appropriate security and technology expertise.*

☐ *The committee should schedule regular meetings with the CFO and internal audit.* It should also have regular meetings and reports from the chief information officer (CIO) and chief information security officer (CISO).

☐ *Create a clear plan outlining the security needs and appropriate standards for your business sector.* For example, in retail, the credit card PCI standard is applicable. What are the backup systems and service levels that are needed for your business? Who has the right to audit the security system? What policies are in place in the event of a breach? How is sensitive data handled, destroyed and accessed? What best practices are recommended?

Boards may groan about the potential cost of seeking outside consulting expertise, but I have found the very best cyber-security experts top out at around $350 per hour.

Outside auditors perform independent audit oversight of company financials and control systems. So too a security and technology committee should have outside experts regularly come in to access and check the companies security practices. This is often call "ethical, white or gray hat" hacking.

While managers (and even the board) may groan about the potential expenses of such expertise, I have found the costs to be negligible. Boards are used to huge price tags for services—multimillion-dollar consulting fees from McKinsey, or corporate attorneys charging $1000 per hour. Yet I have found the very best cyber-security experts typically top out at $350 per hour—a bargain for the value they provide.

Security and technology assets are critical to a company's value protection. The board needs to work with management and review their proposals on the appropriate budget needed for a robust security structure. It is good value to invest in outside consulting to tell you what is wrong with your data security, an even better bargain is to invest in making your internal capability strong in the first place.

As part of your committee's ongoing security and technology work, there should be a regular review

of the number of attacks and incidents that occur, and the effectiveness of the company's response plan. You need a documented recovery policy that identifies processes to inform customers, the general marketplace, and government authorities in the event of a breach. For example, the CIO and CISO could present their vendor selection decisions to the committee for review just as the board reviews other capital expenses on major enterprise resource planning software.

There are many resources that the board can look to for information on how to set up this new committee. For example, a government agency called the National Institute of Standards and Technology (NIST) publishes a well-accepted set of best practices on cyber security. The NACD (National Association of Corporate Directors) in 2014 prepared recommendations for boards in overseeing cybersecurity issues.

It is crucial that the board require management to present their policies on cyber security. This is important for proper board oversight of management's plans on responding in the event of a breach. An oil or chemical company must have an emergency plan in the event of a spill. Likewise, the board should ask management what their plan is in the case of a security breach.

Request that management write up their security practices and standards, and their protocol for responding to a security breach. The board should be able to identify the manager responsible by title, and in what time frame they are to respond to an intrusion.

In the event of a cyber breach, the board should schedule an update from the security committee on any forensic review. This update should identify what the investigation found, and should offer good documentation of any diligence done, and potential liability or reporting issues. For example, there is a Florida "information protection act" that could be violated if a breach impacts state residents. There might also be interstate legal conflicts, and there will be a need to notify the effected agencies.

There may well be other disclosure requirements. The company may need to disclose any data breach in SEC filings if the breach was material. There could even be disclosure requirements for an attempted breach. Your board might be surprised to find out that a court considers failure to disclose a cyber attack as a "material omission," according to some interpretations of new SEC guidance on disclosure.

Finally, in the annual review of your directors and officers (D&O) policy, your board should specifically consider additional insurance for liability related to security privacy and cyber risks. Ask your general counsel and CFO, when reviewing the annual D&O coverage, to see if any new provisions or indemnifications should be added to protect directors from a cyber liability exposure.

My personal boardroom experience on this can be instructive. I served as an outside director with the board of a direct-to-consumer software company a few years back, one that powered 40,000 websites.

When we had a security breach, I asked management for a full forensic investigation. I wanted the board to know who had attacked us, and why, and what the short- and long-term implications would be. What steps would we be taking, and what new programs, policies, procedures would be required. I asked the chief information officer, the head of R&D, the CIO, and CFO to report quarterly to board. We held an emergency board call the day after the breach, another call a week later, and then a live present at the next board meeting.

Our board also told management we wanted someone from outside to make a forensic review. Management's initial response was that they could fix this themselves, but our board said no. We wanted an outside expert to help. One result of this close board follow-up was pretty good containment of the damage. The intrusion ended up costing the company less than we thought. ■