paloalto NETWORKS®

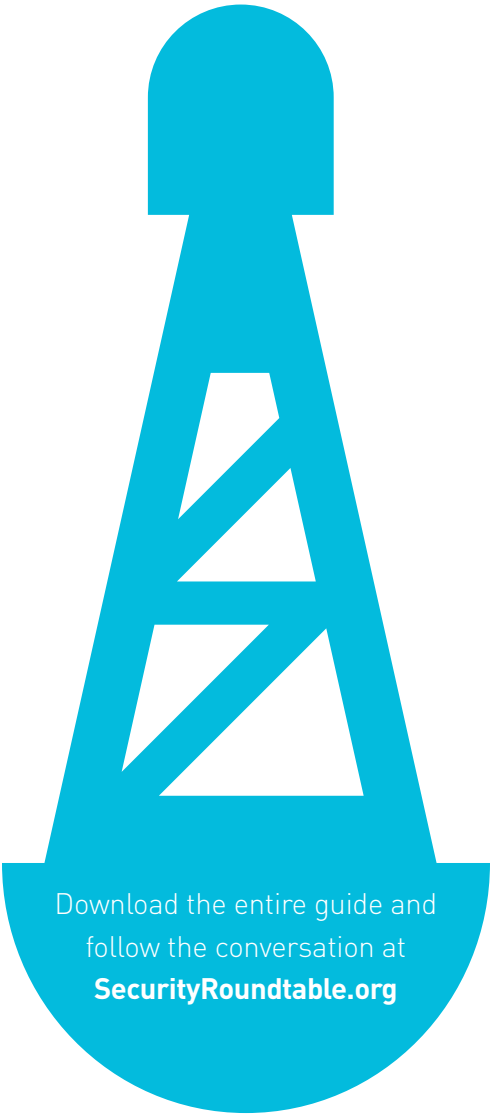
NYSE

NAVIGATING THE DIGITAL AGE

THE DEFINITIVE CYBERSECURITY GUIDE FOR DIRECTORS AND OFFICERS

Georgia Tech Institute for Information Security & Privacy

INTERNET SECURITY ALLIANCE


Download the entire guide and
follow the conversation at
SecurityRoundtable.org

45

Building a cyber-savvy board

Korn Ferry – Jamey Cummings, Senior Client Partner; Joe Griesedieck, Vice Chairman and Co-Leader, Board and CEO Services; and Aileen Alexander, Senior Client Partner

Given the growing magnitude and frequency of cybersecurity breaches, which have the potential to shake major corporations to their core, cybersecurity has become an issue of enterprise-wide importance. These incidents have become commonplace events, and organizations that are targets may suffer lost or stolen intellectual property, damage or destruction of critical data or infrastructure, disruptions to critical operations, and loss of confidence among customers, investors, and employees. The longer-term damage to value and reputation is incalculable.

Startling statistics

PwC's Global State of Information Security Survey 2015 of more than 9,700 security, IT, and business executives found that the total number of security incidents detected by respondents climbed to 42.8 million this year, an increase of 48% over 2013. That is the equivalent of 117,339 incoming attacks per day, every day. The Identity Theft Resource Center reported a record high of 738 U.S. data breaches, a 28% year-over-year increase.

If you're thinking you can build a modern-day "moat" to keep the bad guys out, consider that the 2014 U.S. State of Cybercrime Survey, co-sponsored by PwC, CSO magazine, the CERT Division of the Software Engineering Institute at Carnegie Mellon University, and the U.S. Secret Service, found that almost one-third of respondents said insider crimes are more costly or damaging than incidents perpetrated by outsiders. In a virtual ecosystem that increasingly includes the Internet of Things (IoT), traditional firewalls do not ensure protection, as employees come and go each day with connected devices, such as smartphones and computers, which may wittingly or unwittingly introduce threats that can threaten the survival of the organization.

This greatly expanded cyberattack surface and resulting breaches add up to a huge price tag. The annual cost of cybercrime to the global economy is estimated to be between $375 billion and $575 billion, according to a June 2014 study by the Center for Strategic and International Studies; Gartner Inc. estimates that total spending will grow 8.2 percent in 2015 to reach $76.9 billion.

If that's not a wake-up call, we don't know what is. But, the challenge remains: translating awareness into an action plan. Although CEOs and boards are alert to the issue and the devastating, long-lasting effects of security breaches, there is surprisingly little knowledge of recommended practices to best position organizations defensively and enable quick and effective response when the inevitable occurs. Let's be blunt: There is no foolproof way of preventing security breaches, but a systematic, proven approach can make the difference between the survival and the demise of an enterprise.

Alignment at the top

Cybersecurity is an insidious threat, all the more so because breaches, including the most disastrous ones, often are not detected until the damage is done. One cybersecurity firm recently estimated that close to three quarters of security breaches go undetected. No board or management team can afford to become complacent. If you haven't yet fallen victim, you may have been smart, but most likely lucky. You should assume it's just a matter of time, perhaps there already has been a breach that has gone undetected, so plan accordingly.

In a relatively short time cybersecurity has gone from something that was compartmentalized and handled by the IT department to something that is regularly on the agenda at board meetings. At the same time "major threats" have been redefined, from identifying a Trojan horse and upgrading anti-virus software to threats that strike at the very heart of organizations and are capable of taking them down. The view and importance of cybersecurity has shifted from something of marginal interest to the board to a high priority that resides within the board's risk management framework.

This is a new role for CEOs and directors, many of whom feel unequipped to deal with it because cybersecurity does not remotely relate to traditional areas of director expertise. Armed with a tested protocol to combat cyberthreats and the right resources, however, every board should be able to implement a preparedness and response plan that will give the board and management team, as well as investors, the reassurance that the company is as well positioned as reasonably possible to confront these ever-evolving challenges.

In practical, operational terms, what does all this mean for the C-suite and the board, and how can they get started on overseeing the many-headed beast that is cybersecurity? For one thing, it starts with ensuring everyone on the board is speaking the same language when it comes to cyberthreats. Because directors are generally business people, the common language should be the language of business.

The right questions

According to Melissa Hathaway, private sector cybersecurity expert and former cybersecurity "czar" under Presidents George W. Bush and Barack Obama, "Until cybersecurity is reflected in balance sheet terms, it's never going to be fully embraced by the board." She emphasizes that once cybersecurity has been identified as a critical risk, it must be managed with the same rigor and processes applied to other risks and remain visible on directors' dashboards with key, comprehensible metrics. "Tech speak," or any jargon that obfuscates the issues for directors, has no place in the boardroom.

The reality of boardrooms, however, is that the scale of that impact is often obscured or lost in translation. Unless directors can cut through the technical jargon in what are often massive amounts of information they receive, the size of the risk and the steps to

mitigate it may not be clear. Companies depend on a functioning Internet, which was never invented with security in mind, and all that is linked to it. Therefore, related risks and costs must be made known to the board so that the cost of potential breaches can be calculated in capital and operational terms, rather than remaining hidden.

Among the questions directors should be asking regularly to ensure alignment as a team and a firm grasp on cybersecurity, says Hathaway, are the following:

- **Is cyber risk accounted for in our overall corporate planning process?** The board must be assured that cyber risk is an element of a broader risk framework and that exposures are recognized and planned for.
- **What is the process for evaluating security and measuring liabilities?** Boards should know not only what controls are in place but also how they are evaluated.
- **Do we have directors with relevant expertise?** Although boards may not require general technology expertise, it may be advisable to have one or more directors who understand IT and its associated risks, or have a security background.
- **Have we identified executive ownership of the issue?** The CEO should have controls in place that indicate how cybersecurity is being managed and the true costs to the business, which should be part of an internal and external audit.
- **What will we do in the event of a breach?** If and when a problem arises, a process should be in place for communicating effectively, internally and externally, and dealing with attendant costs.

Overseeing cyber risk

Boards are increasingly adding directors with cybersecurity backgrounds and, more generally, security expertise, but boards should not assume that they need to add a director with this specialized background. Much depends on company specifics and the industry in which it operates, so each board should decide on a case-by-case basis. Shortfalls in board experience often can be made up by retaining the appropriate additional expertise to advise on an as-needed basis; however, we are starting to see more demand for this specific sort of talent on boards.

Sometimes, as noted above, the board's most important role lies in asking the right questions, which may require business smarts and good old-fashioned common sense but not necessarily technical cybersecurity expertise.

As overseer-in-chief of the CEO and the business, the board has a responsibility for managing the company's risk portfolio, of which cybersecurity is now a key component. Proper oversight entails remaining at a high, supervisory level—not getting dragged down into the management weeds—and boards can properly perform their fiduciary duties by focusing on a few main areas.

The board must be reassured by the CEO that the most capable people are in the critical positions, and this extends to the leadership and team managing cybersecurity. With so much at stake, this is not a place to cut corners.

Directors should be kept abreast of main cybersecurity risks, as well as the remediation process and timeline for effectively dealing with them. Certainly no one expects directors to be technology wizards, but they should be inquiring about safeguards the company has in place to guard against intrusion and be satisfied by management that protection along with response and recovery capabilities are adequate. In addition, they will want to be informed about education for everyone throughout the organization, to ensure awareness of threats, and a step-by-step response plan to follow in the event of a breach.

The board at the nexus

Cybersecurity has expanded well beyond the confines of IT and emerged as a concern at the highest enterprise level, primarily because of the devastating potential effects

on shareholder value, market share, reputation, and long-term survival. Cybersecurity is an issue that crosses all organizational silos and boundaries top to bottom, encompassing people, culture, and risk management and must bridge security, technology, privacy, and compliance. Cybersecurity is, therefore, taking its rightful place on a short list of the board's crucial responsibilities, which now include protecting a company's assets, particularly digital, as part of an organization's overall risk portfolio.

In fact, managing cyber risk doesn't differ significantly from managing more traditional forms of risk and must be managed in a similar way, remaining visible on directors' dashboards so that it is tracked and addressed regularly.

Those boards that do not have a cybersecurity expert as a member of their team should not assume they need a director with this experience, but they should seriously evaluate that potential need based on their situation and needs. Some boards have determined that they do require this expertise on their audit committee—where risk oversight generally lives—on a special cybersecurity subcommittee, or on a dedicated cybersecurity committee. While some boards have recruited this expertise, many have not and may not, accessing what they require to keep them informed and able to make key decisions either from internal technology experts or from external consultants to the board. These solutions are varied and tailored and continue to evolve.

CEOs and those who serve as directors on their boards are generally a smart group of people, and they don't have to be subject matter experts to provide oversight for the few crucial areas—including strategy formulation, succession planning, and risk management—in which they exercise their fiduciary duties. Cybersecurity is yet another form of risk, but it is a dynamic, still-emerging form that is new to most directors. We are likely years away from the point where boards as a whole consider managing cyber risk familiar terrain, so additional resources can always be made available should directors need bolstering in this area.

In fact, directors owe it not only to their shareholders to ensure a comprehensive approach to monitoring and developing a proactive approach to tackling cybersecurity but also to themselves. With cybersecurity in the spotlight—where it is likely to remain—directors could also face personal risks, because D&O insurance may not be sufficient if boards don't take what are deemed appropriate actions. Boards should consider adding cyber insurance as part of a comprehensive approach to enterprise risk management if they are to continue to recruit the best directors. According to a recent post on the Harvard Law School Forum on Corporate Governance and Financial Regulation, "no company in the U.S. should forego buying cyber insurance to protect against the real, ever-present risk of a major cyber-attack and the massive costs associated with such a breach."

A framework to meet the cybersecurity challenge

Perhaps most important in properly meeting the cybersecurity challenge, ensuring preparedness and a ready response to any breaches, directors need a framework, which can be tailored to the needs of their organization, in which to operate. A deep dive into each area will link to additional responsibilities and timeframes, most of which will be the responsibility of management.

The baseline for board involvement in overseeing cybersecurity should comprise the six following components:

1. **Security strategy.** The board must ensure that the company has a strategic vision and a tactical road map that proactively protect assets and keep pace with escalating threats and evolving regulatory requirements.
2. **Policy and budget review.** Company security policies, and roles and responsibilities of all relevant leadership, should be evaluated, along with data

security and privacy budgets to ensure they are adequately funded.

3. **Security leadership.** The board must confirm that the organization has the credible leadership and talent to develop, communicate, and implement an enterprise-wide plan to manage cyber risk.
4. **Incident response plan.** The board should oversee the development of a comprehensive incident response plan that is widely understood, rehearsed, and stress tested.
5. **Ongoing assessment.** The board should periodically review a thorough assessment of the organization's information security capabilities, targeting internal vulnerabilities and external threats.
6. **Internal education.** The board should ensure that the company implements a strong communication and education program to create an environment in which all employees embrace responsibility for cybersecurity.

A cybersecurity strategy

Organizations must have a cybersecurity strategy, lest they simply be engaged in a game of whack-a-mole, reacting to one threat after another rather than having a comprehensive game plan. That is not to say that cyberthreats and breaches can be eliminated—clearly they cannot—but the resulting damage can be greatly minimized with significant planning and a quick response protocol.

In part, effectively managing cybersecurity starts at the top with the board recognizing what it must manage and how that will be done, including additional resources it may require. While the board may have ultimate responsibility for the war on cyberthreats, everyone, at every level of the organization, must understand his or her role on the front lines of this ongoing war, because threats can come from anywhere.

Moreover, in an increasingly robust regulatory environment with cybersecurity high on the SEC's agenda, adherence to best practices with a well-designed plan approved and monitored by the board should prove far preferable to regulations imposed from the outside. Given the current direction, in the near future it is likely that publicly owned companies will be required to disclose more information about their cybersecurity vulnerabilities, including data breaches.

Ultimately, boards should work with senior management to build a cybersecurity-aware culture if they are to truly protect their companies from this relatively new, continually morphing, and potentially devastating form of risk.

Korn Ferry

2101 Cedar Springs Road
Suite 1450
Dallas, Texas 75201
Tel +1 214 954 1834
Web www.kornferry.com

AILEEN ALEXANDER

Senior Client Partner
Email aileen.alexander@kornferry.com

Aileen Alexander is a Senior Client Partner and co-leads Korn Ferry's Cybersecurity Practice. Based in the firm's Washington, D.C., office, she has led senior executive searches across the security domain. She also partners with the firm's Board & CEO Services practice.

In a previous position with another international executive search firm, Ms. Alexander served clients in the aerospace and defense and professional services sectors.

Prior to the talent management profession, Ms. Alexander was a Professional Staff Member on the Committee of Armed Services in the U.S. House of Representatives. Previously, she was a Presidential Management Fellow in the Office of the Secretary of Defense and served as a Captain in the U.S. Army.

Ms. Alexander holds a master's degree in public policy from Harvard University's Kennedy School of Government and earned a Bachelor of Arts degree from The Johns Hopkins University.

JAMEY CUMMINGS

Senior Client Partner
Email jamey.cummings@kornferry.com

Jamey Cummings is a Senior Client Partner in Korn Ferry's Global Technology and Information Officers Practices, and he co-leads the firm's Global Cybersecurity Practice. Based in the firm's Dallas office, he is also a member of the firm's Aviation, Aerospace & Defense Practice.

Prior to Korn Ferry, Mr. Cummings served as an associate principal in the industrial, supply chain, and transportation and logistics practices of another leading executive search firm, where he executed executive search assignments for public and private equity-backed companies.

Earlier in his career, Mr. Cummings was a consultant with The Boston Consulting Group in Dallas and, before that, he served nine years with distinction as an officer in the U.S. Navy's SEAL teams.

He earned a master's degree in business administration from Stanford University and graduated with merit with a bachelor of science in aeronautical engineering from The United States Naval Academy.

JOE GRIESEDIECK

Vice Chairman & Co-Leader, Board & CEO Services
Email joe.griesedieck@kornferry.com

Joe Griesedieck is Vice Chairman and Co-Leader, Board and CEO Services at Korn Ferry. He focuses primarily on engagements for board director searches across multiple industries, as well as working with boards of directors on succession planning and other related senior talent management solutions.

Mr. Griesedieck's prior experience includes two terms as global chief executive officer of another international search firm. He also served as co-head of the firm's strategic leadership services practice in North America.

Prior to entering the executive search profession, Mr. Griesedieck was a group vice president with Alexander & Baldwin, Inc., and spent a number of years with the Falstaff Brewing Corporation, concluding his tenure as president and chief operating officer and as a director of this NYSE company.

Mr. Griesedieck has been named by The National Association of Corporate Directors (NACD) to the Directorship 100, recognizing the most influential people in corporate governance and the boardroom.

Mr. Griesedieck is a graduate of Brown University.