ISSUE 101

protiviti®
Face the Future with Confidence

Board Perspectives:
Risk Oversight

The Cyber Risk Oversight Challenge

Every board today faces the challenge of overseeing the investment of finite protection resources in an ever-changing cyber threat landscape. Our recent discussion with a group of active directors identified some interesting cyber-related topics germane to board oversight.

Cybersecurity is likely to remain centre stage as a top risk as companies continue to expand their reliance on digital technologies to transform customer experiences and execute global growth strategies. In a recent global survey from Protiviti and North Carolina State University's ERM Initiative,[1] more than 700 directors and C-level executives ranked cyber risk as a top three risk overall, and a "significant impact" risk for businesses in financial services; technology, media and communications; health and life sciences; and energy and utilities. Both directors and CEOs rated cyber as the second-highest risk.

Companies today fall into two groups — those that have been breached and know it, and those that have been breached but *don't* know it. The realities of managing cybersecurity risks are that they are impossible to eliminate, resources for managing them are finite, risk profiles are ever-changing and getting close to secure is elusive. Furthermore, organisations need IT resources to innovate so they can remain competitive; as important as the cyber imperative is, directors should not allow it to dominate the IT budget and stifle innovation.

In December 2017, Protiviti met with 18 active directors during a dinner roundtable at a National Association of Corporate Directors (NACD) event to discuss the board's cybersecurity oversight. Rather than go over well-travelled topics such as targeting finite protection measures on the organisation's "crown jewels" and systems availability, understanding the ever-changing threat landscape and related risk tolerances, and preparing for inevitable incidents, this group of directors identified some other interesting insights into cyber risk oversight at the board level. Following are the topics we discussed.

[1] *Executive Perspectives on Top Risks for 2018*, Protiviti and North Carolina State University's ERM Initiative, December 2017, available at www.protiviti.com/toprisks.

Winning Battles Does Not Necessarily Win the War

The discussion focused on how state-sponsored attacks targeting government institutions, industrial facilities, infrastructure and many business organisations are increasing in both power and sophistication. Combatting so-called advanced persistent threats (APTs) effectively requires faster detection and more advanced response tactics. But most U.S. organisations seem to be operating from a 1990s playbook when it comes to cyber, while aggressor nation-states, such as China, appear to be using a 2050 playbook.

What makes APTs especially dangerous is that they can adapt to an entity's preventive countermeasures. They can also change the paths by which they infiltrate a computer or network server to deliver malware payloads that may be altered over time. Stealth is the goal, as an APT may either seek to cover its tracks once its objectives are achieved or lie dormant for an indeterminate period for activation later at an appointed time or in a designated situation.

In the arms race to keep pace (or, in most cases, catch up) with these threats, need to commit themselves to tapping into available government intelligence and using it to facilitate their preparedness. Directors should suggest the management team develop and maintain relationships with the correct contacts in the government sector needed to stay informed of emerging risks. For example, as attacker resources and sophistication have increased over time, regulators and various government agencies in the United States have formed an information sharing and analysis centre (ISAC) for multiple industries. An ISAC is a nonprofit organisation that provides a central resource for gathering and sharing information on cyber threats to critical infrastructure. There is so much information provided that companies should allocate adequate resources to monitor it over time and determine what actions to take to address new and emerging threats.

Upgrading Detection Capabilities

The directors raised concerns over the maturity of most companies' countermeasures and what can be done at the board level to encourage more effective mitigation of the risks. If management and the board believe the entity is an APT target based on what it represents, what it does and the intellectual property it owns, the organisation's cybersecurity capabilities need to be upgraded beyond the controls, tools and response mechanisms traditionally used to contain sophisticated attackers and corporate insiders. Our experience is that detective and monitoring controls remain immature across most industries relative to the evolving threat landscape, resulting in continued failure to detect breaches promptly.

Simulations of likely attack activity should be performed periodically to ensure defences can detect a breach and security teams can respond swiftly. However, our experience with such simulations is that, too often, clients authorising the testing fail to detect our test activity. Contrary to what many executives think, outsourcing to a managed security service provider does not solve the problem, as we often see breakdowns in the processes and coordination between the company and service provider that result in attack activity not being detected. If an advanced attacker enters a systems environment in which detective controls have repeatedly failed to detect breach activity in a timely manner, it's game over.

Clarifying Expectations With Management

One director noted that when a chief information officer (CIO) or chief information security officer (CISO) asserts, "Don't worry, we're taking care of that," or delivers a similar pushback, it tends to stifle the dialogue and leaves directors with nowhere to go and an incomplete understanding of cyber risk mitigation. The group's ensuing discussion pointed to several themes:

- **Ask the right questions —** It's important for boards to ask the right questions about situational awareness, strategy and operations, insider threats, incident response, and other related topics. (An appendix in the 2017 NACD publication on cyber risk oversight suggests relevant questions.[2])

[2] See Appendix A, *NACD Director's Handbook Series on Cyber-Risk Oversight*, NACD, 2017, available for purchase at www.nacdonline.org/Store/ProductDetail.cfm?ItemNumber=10687.

- **Consider changing board composition —** If the board could benefit from more IT and security expertise, there may be a need for a technology expert: either a director on the board or an objective third party advising the board. Boards tend to bring on "business people" as members; therefore, it might be worth considering bringing on members (and/or advisers) with the requisite technology background.
- **Establish a separate cybersecurity or technology committee of the board —** This is always an option, depending on the severity of the threat landscape and the role of technology in executing the company's business strategy.

Although directors have limited time to get into details, they should set clear expectations for management at all levels with respect to cyber incidents that can affect the company's reputation, brand image and standing with customers. Expectations regarding cybersecurity strategy and risk tolerances should be incorporated into the entity's risk appetite statement.

Improving Board Cybersecurity Reporting and Metrics

The severity of the Equifax breach as well as others raises the question as to whether boards are probing deeply enough to determine what they don't know. To that end, the directors noted that, too often, board reports deliver high-level information only. So, the question then becomes, what reporting and metrics on cybersecurity should the board request? The discussion pointed to several key areas to consider:

- **The number of system vulnerabilities —** Management should identify high-risk system vulnerabilities and report changes over time. Is the board satisfied with how management identifies, quantifies and prioritises vulnerabilities?
- **The length of time required to implement patches —** The typical time window for patching known high-risk system vulnerabilities is 60 to 90 days. Thirty days is generally considered the "gold standard," but even that is too long in some instances.[3]
- **The length of time to detect a breach —** With respect to the elapsed time between the initiation of an attack and its ultimate discovery, our experience is that the average length of time to detect is six months — a considerable amount of time given the risks.
- **The length of time to respond to a breach —** Is the board satisfied with the elapsed time between the discovery of a security breach and the initiation of the response plan to reduce the threat's proliferation and impact?
- **The length of time to remediate audit findings —** With respect to third-party or in-house audit recommendations to improve cybersecurity, the board should monitor remediation of high-risk audit findings, including the time it takes to complete the remediation process.
- **Percent of breaches perpetrated through third parties —** Based on our experience, on average, 50 percent of breaches occur at an organisation's vendors rather than the organisation itself — a staggering statistic that warrants attention.
- **The number of security protocol violations —** Management should measure violations of security policies and procedures across the organisation and report trends in violations over time to indicate whether there has been progress toward improving cybersecurity.

While not exhaustive, reporting on the above metrics can inform the board's cyber risk oversight. Interestingly, one director noted that when the board asks management for more reporting on anything, exceptions tend to go down. Cyber is no exception. In setting the tone for management, the board should ensure it can view results and outcomes with a focused dashboard. To that end, the 2017 NACD publication on cyber risk oversight includes examples of cyber risk reporting metrics and dashboards.[4]

However, directors should use dashboard reporting with caution. Management tends to provide a lot of data, but the board needs to dig deeper to determine what it doesn't know. For example, if there is a metric around the volume of data the organisation is

[3] "How Long Does It Take to Implement a Patch?" *Board Perspectives: Risk Oversight*, Issue 97, Protiviti, November 2017: www.protiviti.com/US-en/insights/bpro97.

[4] See Appendices E and F, *NACD Director's Handbook Series on Cyber-Risk Oversight*, NACD, 2017, available for purchase at www.nacdonline.org/Store/ProductDetail.cfm?ItemNumber=10687.

managing and protecting, deeper questions should be asked about whether that data is encrypted. Consider that a health insurance plan provider lost unencrypted data because its data was only encrypted in transit rather than at rest — a nuanced reason it ended up having almost 80 million records accessed.

Paying Attention to "Blocking and Tackling"

During our discussion, the group brought up several "blocking and tackling" issues related to cybersecurity, including:

- **Prioritising high-risk patches —** With patching vulnerabilities now squarely in the line of sight of many boards, the directors noted that the patch process is sometimes viewed as a "silo" issue. The consensus view: Management needs to get a better handle on this issue to ensure the organisation is addressing these matters quickly and aggressively.
- **Inquiring about multifactor authentication —** One director noted that every organisation should have this computer access control in place. Accordingly, the board should discuss this security measure with management.
- **Raising awareness of phishing —** The key is not how many phishing emails the organisation receives (a metric that may be presented in the dashboard), but rather how many users in the company are duped by this tactic — and how the organisation responds. For example, an appropriate response might be that all people who open a phishing email attend security training.
- **Implementing security segmentation —** Regulators expect organisations to segment data so that malicious actors who infiltrate networks and systems cannot access everything. Segmentation is vital to protecting critical data and the crown jewels if access controls are compromised.
- **Refreshing incident response and recovery plans continuously —** The point was made that most post-breach business continuity plans fall short — often because the plans are outdated. The board therefore needs to discuss with management the adequacy of the organisation's incident response and business continuity plans and monitor the follow-up to such discussions.

Conducting Independent Cybersecurity Assessments

Innovative transformation initiatives are constantly expanding an organisation's digital footprint. They also outpace security protections companies have in place, producing a sobering reality: Security and privacy internal control structures that are effective in reducing cyber risk to an acceptable level today will inevitably become inadequate, perhaps sooner than management realises.

Even more sobering is that the solutions management represented to the board as "effective" a year ago may be inadequate today. That is why organisations should consider assessing the current state of their overall cybersecurity using an established framework,[5] so they can identify and prioritise opportunities for improvement in pursuing their desired state. If such reviews identify gaps or areas of weakness requiring immediate remediation, the board should satisfy itself that management addresses those areas in a timely manner.

Being Aware of Challenges in the Information Technology (IT) and Security Organisations

During our roundtable discussion, the point was raised that many organisations are not built to address current cyber threats. Accordingly, they need to seriously consider re-architecting themselves from both a technology and security standpoint. In short, they need to change how they do things. So, the question the board needs to ask management is: How quickly are we able to get an issue resolved? Management assertions that a solution will disrupt existing operations and legacy systems and, thus, will take time to implement, are a red flag.

Our discussion also touched on the issue of inadequate IT and security resources. The reality of finite resources is that organisations must target them appropriately to the data and information systems assets that matter. But management often is not proactive enough on this front, especially if the organisation has not had a serious breach or security issue. Many companies simply don't know what they don't know, and that makes it tough for management to prioritise IT resources for cybersecurity. The need to

[5] An example of such a framework is the National Institute of Standards and Technology (NIST) Cybersecurity Framework. For more information, see www.nist.gov/cyberframework.

innovate is another complication. Protiviti's research indicates that mature businesses are able to devote only about 13 percent of their IT budgets to innovation today, reflecting a decline over the past decade.[6]

Considering the Value of Cybersecurity Insurance

One director brought up the importance of cyber-security insurance coverage as a means to transfer some of the financial risk associated with a variety of cybersecurity incidents, including data breaches, business interruption and network damage — particularly since the entity's directors and officers liability policy may not cover these issues.

If a company invests in a cybersecurity policy, the insurer may require the business to follow certain guidelines and provide evidence through a cybersecurity assessment, as discussed earlier. If the company hasn't benchmarked itself against an appropriate framework, directors should inquire as to why not; it may be important for reducing the cost of cybersecurity insurance.

Questions for Independent Directors

Boards of directors may want to consider the following questions in the context of the nature of the entity's risks inherent in its operations:

- Is the company a possible nation-state target based on what it represents, what it does or the value of its IP? If so:
  - Does the company have the advanced detection and response capabilities it needs?
  - Are simulations of likely attack activity, given the increasing sophistication of likely threat actors, performed periodically to ensure defences can detect a breach and respond in a timely manner?
  - Does management assess cybersecurity maturity against a suitable framework in view of its threat environment and follow up on areas in need of improvement?
- Does the board define its cyber expectations for management and establish clear accountabilities for results? If the organisation has a risk appetite statement, are the board's expectations for cybersecurity incorporated therein?
- Is the board satisfied with the reporting and metrics used by management on cyber matters? Do the metrics provide key performance and risk indicators addressing how top cyber risks are managed and areas that inform the board's oversight, including the example metrics and the "blocking and tackling" issues noted above?
- Is the board satisfied that an effective response and recovery plan is in place? Is the plan evaluated through tabletop exercises, tested periodically and adjusted as the threat landscape, people, systems and business processes change?
- Is sufficient IT budget available to support innovation? If not, is the spend on operational risk proportionate and focused on protecting what's important (the "crown jewels"); keeping up with the cyber threat landscape to identify the kinds of attacks that are most likely to occur; and being proactive about incident response so systems can be put back online with minimum impact to the business?

[6] *From Cloud, Mobile, Social, IoT and Analytics to Digitization and Cybersecurity: Benchmarking Priorities for Today's Technology Leaders,* Protiviti, November, 2016: www.protiviti.com/sites/default/files/united_states/insights/annual-technology-trends-and-benchmark-study-2016-protiviti.pdf.

How Protiviti Can Help

Protiviti works with organisations to focus on foundational information security questions:

- Do we know what we need to protect (e.g., the data and information systems assets that are most important — the crown jewels) and where they are located? Regarding these assets:
  - Are we properly caring for them? How do we know?
  - Who are we protecting them from, to whom should we permit access, and how can we tell the difference?
  - Do we have effective defences in place? Are they working as designed?
  - How will we know if things are not working as we planned?
- Are we able to recognise a new threat to our environment and detect likely attack techniques on a timely basis and align our protection measures to meet the threat?
- Are we ready to respond if something bad happens? Are we capable of managing such incidents? When incidents occur, are we able to keep them from happening again?

Protiviti provides a wide variety of security and privacy assessment, architecture, transformation, and management services to help organisations identify and address security and privacy exposures (e.g., loss of customer data, loss of revenue or reputation impairment) before they become problems. Working with companies in all industries, we evaluate the maturity of their information security programs and the efficacy of their controls — and help them design and build improvements when needed.

We have a demonstrated track record of helping companies react to security incidents, establish proactive security programs, deal with identity and access management, and handle industry-specific data security and privacy issues. Our experience and dedication to developing world-class incident response have resulted in deep expertise in security strategies, response execution, forensic analysis and response plan development.

Is It Time for Your Board to Evaluate Its Risk Oversight Process?

The TBI Protiviti Board Risk Oversight Meter™ provides boards with an opportunity to refresh their risk oversight process to ensure it's focused sharply on the opportunities and risks that truly matter. Protiviti's commitment to facilitating continuous process improvement to enable companies to confidently face the future is why we collaborated with The Board Institute, Inc. (TBI) to offer the director community a flexible, cost-effective tool that assists boards in their periodic self-evaluation of the board's risk oversight and mirrors the way many directors prefer to conduct self-evaluations. Boards interested in using this evaluation tool should visit the TBI website at http://theboardinstitute.com/board-risk-meter/.

Learn more at
www.protiviti.com/boardriskoversightmeter

Protiviti is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independently owned Member Firms provide consulting solutions in finance, technology, operations, data, analytics, governance, risk and internal audit to our clients through our network of more than 70 offices in over 20 countries.

We have served more than 60 percent of *Fortune* 1000® and 35 percent of *Fortune* Global 500® companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

Protiviti partners with the National Association of Corporate Directors (NACD) to publish articles of interest to boardroom executives related to effective or emerging practices on the many aspects of risk oversight. As of January 2013, NACD has been publishing online contributed articles from Protiviti, with the content featured on https://blog.nacdonline.org/author/jdeloach/. Twice per year, the six most recent issues of *Board Perspectives: Risk Oversight* are consolidated into a printed booklet that is co-branded with NACD. Protiviti also posts these articles at protiviti.com.

protiviti®