ISSUE 90

protiviti®
Face the Future with Confidence

Board Perspectives:
Risk Oversight

Board Oversight of Cyber Risk

Boards remain concerned with the security and availability of information systems and the protection of confidential, sensitive data from the commercial cyber war in which their organisations are engaged. Many executives think their risk tolerance is low, yet act as though it is relatively high, thus necessitating board engagement with cybersecurity.

A top five risk for many organisations across many industries,[1] cyber risk presents a moving target as organisations undergo major IT transformations, accelerate cloud computing adoption, increase digitisation investments,[2] advance data and analytics sophistication, and expand mobile device use to leverage exponential increases in computing power for competitive advantage. As these innovative IT transformation initiatives keep expanding the digital footprint, they outpace the security protections companies have in place. This dilemma presents a sobering reality: Security and privacy internal control structures that are effective in reducing risk to an acceptable level today will inevitably become inadequate in the future — and even sooner than many may realise. In fact, organisations already may be breached and not know it. Boards of directors need to ensure that the organisations they serve are improving their cybersecurity capabilities continuously in the face of ever-changing cyber threats.

Key Considerations

Our research indicates that board engagement in information security matters is improving.[3] In the spirit of further improvement, following are eight business realities directors should consider as they oversee cybersecurity risk:

1. **The organisation must be prepared for success.** Managing cybersecurity is not just about managing the risk of bad things happening, it's also about handling the upside of a company's successful digital initiatives. As companies harvest new sources of value through digitisation and business model innovation, more progress is needed to mature the performance of security and privacy capabilities across the enterprise. The wise course is to plan for incredible success. Directors should ensure that the organisation's cybersecurity policies and systems are resilient enough to handle that success.

[1] *Executive Perspectives on Top Risks for 2017*, Protiviti and North Carolina State University's ERM Initiative, 2017, available at www.protiviti.com/US-en/insights/protiviti-top-risks-survey.

[2] "Digitization" is the process of converting analog source material to digital form with the objective of improving business processes.

[3] *Managing the Crown Jewels and Other Critical Data*, Protiviti, 2017, available at www.protiviti.com/US-en/insights/it-security-survey.

2. **It is highly probable that the company is already breached and doesn't know it.** The old thinking of "it's not a matter of if a cyber risk event might occur, but more a matter of when" is dated. It's happening — now. For most companies, cyber risk events have already happened and may still be underway. Yet many organisations do not have the advanced detection and response capabilities they need. The proliferation of data privacy regulations around the globe and the publicity about data breaches affecting politicians, governmental agencies, global financial institutions, major retailers and other high-profile companies, along with the growing presence of state-sponsored cyberterrorism and espionage, are leading directors and executives alike to recognise the need for "cyber resiliency" to preserve reputation and brand image.

   Boards should be concerned about the duration of significant breaches before they are finally detected. Our experience is that detective and monitoring controls remain immature across most industries, resulting in continued failure to detect breaches in a timely manner. Tabletop exercises alone are not sufficient to address the increasing sophistication of perpetrators and the significant impact of a breach. Simulations of likely attack activity should be performed periodically to ensure that defences can detect breaches and responses are timely. In addition, an organisation's preparedness to reduce the impact and proliferation of an event is key. Accordingly, boards should focus on the adequacy of the company's playbook for responding, recovering and resuming normal business operations after an incident has occurred. The playbook should also include responses to customers and employees to minimise reputation damage that could occur in a breach's wake.

3. **The board should focus on adverse business outcomes that must be managed.** Most businesses know what their critical data assets and information systems are, the so-called "crown jewels." However, they forget to focus on the business outcomes they are looking to manage when they assess security risks. Considering risk outcomes or scenarios leads to enterprise security solutions that are more comprehensive than steps taken based on a narrower focus on specific assets and systems.

   To illustrate, once an application is deemed key to the success of the business, it is typically considered "in scope" and managed. If the risk pertains to sensitive data leakage, the security solution is often focused on the source application and implementation of generic security controls. But the risk of an adverse outcome extends beyond the technology perimeter and may be an even greater risk. Users have access to data, regularly download it and might even email it, either ignoring or forgetting the business imperative to protect it. Therefore, controls over what happens to critical data assets once downloaded cannot be ignored. They won't be if user leakage is an integral part of the adverse outcomes to be managed. That's why boards should insist IT leaders look at information security risks holistically, focusing on strategies to manage adverse business outcomes rather than throwing money at addressing every technical weakness.

4. **Cyber threats are constantly evolving.** Because the nature and severity of threats in the cyber environment change incessantly, protection measures must evolve to remain ahead of the threat profile. While recurring assessments are important, they should not be relied on as the sole means to identify new threats to manage. Boards should inquire as to how the organisation's existing threat management program proactively identifies and responds to new cyber threats, taking into consideration the company's crown jewels, the business outcomes it wishes to avoid, the nature of its industry and business model, and its visibility as a potential target. Directors should also insist on an assessment of the related cyber risks resulting from major systems changes. It is always less expensive to build security into a system's design early rather than to retrofit it later.

5. **Cybersecurity is like a game of chess, so play it that way.** IT security organisations must be steps ahead of cyber adversaries, waiting and ready with an arsenal of technology, people, processes and prowess. The old game of sole reliance on technology to deliver an effective and sustainable security monitoring solution falls short time and again when combating the onslaught of ever-changing threats to businesses today. Security functions need to change the way they deliver protective services and move far beyond initiatives to create enterprisewide cyber awareness. Accordingly, boards should expect:

   - A clear articulation of the current cyber risks facing all aspects of the business (not just IT);
   - A summary of recent cyber incidents, how they were handled, and lessons learned;
   - Short- and long-term road maps outlining how the company will continue to evolve its cyber capabilities to address new and expanded threats, including the related accountabilities in place to ensure progress; and
   - Meaningful metrics that provide supporting key performance and risk indicators of successful management of top-priority cyber risks that are being managed today.[4]

   For those organisations facing significant gaps between the current state and the target state in their capabilities for managing security risks, a cybersecurity program office is an emerging practice for managing large security projects successfully with a focus on technology, people and processes aligned with the enterprise's key risks.

6. **Cybersecurity must extend beyond the four walls.** Notable gaps in knowledge of vendors' data security management programs and procedures currently exist between top-performing organisations and other companies — particularly in areas that might stand between an organisation's crown jewels and cyberattackers.[5] As companies look upstream to vendors and suppliers (including second tier and third tier) and downstream to channel partners and customers, they are likely to find sources of vulnerability. Directors should expect management to collaborate with third parties to address cyber risk in a cost-effective manner across the value chain when assessing insider risk because electronic connectivity obfuscates the notion of who constitutes an "insider." As the use of cloud-based storage and external data management vendors increases, the importance of vendor risk management grows.

7. **Cyber issues cannot dominate the IT budget.** Without question, boards should ensure that cybersecurity is appropriately addressed and sufficiently resourced. However, as important as the cyber imperative is, directors should not allow it to stifle innovation. Over the past decade, IT departments have been reducing operations and maintenance costs consistently, funnelling most savings to fund other priorities like security. Taking into account other priorities, including compliance and system enhancements, Protiviti's research indicates that mature businesses are left with only 13 percent of their IT budgets for innovation.[6]

   With a strained budget, it becomes critical for IT leaders to focus on: first 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 that systems can be put back online with minimum impact to the business. Without this discipline, cybersecurity will continue to consume larger portions of the IT budget. Innovation will then suffer, and the business could ultimately fail — not because a cyber threat is realised, but because the disproportionate and unfocused spend on operational risk has distracted the business from the strategic risk of failing to mount a competitive response to new entrants and/or innovators.

[4] Examples of such metrics might include: security program assessment results reflecting current and target maturity; percent of third parties assessed; percent of high-risk business processes reviewed for segregation of duties conflicts; severe vulnerabilities identified and addressed (e.g., number of data leakages with costs to fix); number of high-risk incidents per month; average incident remediation time; status of remediation of identified high-risk audit and regulatory issues (e.g., number of issues closed, open and past established aging thresholds); and percent of employees passing phishing tests.

[5] *Managing the Crown Jewels and Other Critical Data*, Protiviti, 2017, available at www.protiviti.com/US-en/insights/it-security-survey.

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

8. **Directors should gauge their confidence in the advice they're receiving.** While there is no one-size-fits-all solution, boards should periodically assess the sufficiency of the expertise they rely on for cybersecurity matters. There may be circumstances where the board should strongly consider adding individuals with technology experience, either as members of the board or as advisers to the board, especially when the board's agenda is crowded.

Cybersecurity is likely to remain centre stage as a top risk for a long time as companies increase their reliance on new technologies in executing their global strategies. The realities of managing cyber risks are that they are impossible to eliminate, resources are finite, risk profiles are ever-changing, and getting close to secure is elusive. Thus, it is imperative for companies to target protection investments on the business outcomes that can adversely impact the organisation's crown jewels, understand the changing threat landscape and risk tolerances, and prepare for the inevitable incidents.

Questions for Boards

Following are suggested questions that boards of directors may consider, in the context of the nature of the entity's risks inherent in its operations:

- As a board, are we sufficiently engaged in our oversight of cybersecurity? For example:
  - Do we include cybersecurity as a core organisational risk requiring appropriate updates in board meetings?
  - Do we have someone on the board or advising the board who is the focal point for this topic?
  - Are we satisfied that the company's strategies for reducing the risk of security incidents to an acceptable level are proportionate and targeted?
  - Does the board receive key metrics or reporting that present the current state of the security program in an objective manner?
  - Is there a policy on securing board packets and other sensitive material communicated to directors? If not, is there potential exposure from sharing confidential information through directors' personal and professional email accounts and free file-sharing services that are not covered by the company's cybersecurity infrastructure?
- Have we identified the most important business outcomes (both unanticipated successes of the digital initiative, as well as adverse events) involving critical data and information assets (the crown jewels)? With respect to those outcomes occurring:
  - Do we know whether and how they are being managed?
  - Does our security strategy differentiate them from general cybersecurity?
  - Do we assess our threat landscape and tolerance for these matters periodically?
  - Are we proactive in identifying and responding to new cyber threats?
- Does the company have an incident response plan? If so:
  - Have key stakeholders supported the development of the plan appropriate to the organisation's scale, culture, applicable regulatory obligations[7] and business objectives?
  - Have we thought about the impact specific cyber events can have and whether management's response plan is oriented properly and supported sufficiently?
  - Is the plan complemented by procedures providing instructions regarding actions to take in response to specific types of incidents? Do all the stakeholders for a planned response know their respective roles and responsibilities? Is it clear for which events the board should play a key role in overseeing the response efforts?
  - Are effective incident response processes in place to reduce the occurrence, proliferation and impact of a security breach?
  - Are we proactively and periodically evaluating and testing the plan to determine its effectiveness? For example, does management have regular simulations to determine whether the detective capabilities in place will identify the latest attack techniques?
  - In the event of past significant breaches, have we made the required public disclosures and communicated the appropriate notifications to regulators and law enforcement in accordance with applicable laws and regulations?

[7] For example, the Gramm-Leach-Bliley Act for financial institutions and the Health Insurance Portability and Accountability Act (HIPAA) for health information in the United States, and PCI security standards for payment systems.

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? With respect to 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?
  - Are the defences we have put in place effective? Are they working as we designed them to?
  - 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 were to happen? Are we capable of managing such incidents? And 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 education and 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®