Five Questions to Guide Cybersecurity Risk Management

The quick transformation of cybersecurity risk management from obscure specialty to top-of-the-house priority presents an unusual management, governance, and supervisory concern. Executives, board members, and regulators must determine whether technology and cybersecurity professionals have adequately prepared a company for the overall cybersecurity risk it faces. Mounting effective challenge may feel difficult to achieve in an area presumed to be as arcane and complex as cybersecurity posture.

But it doesn’t take an engineering degree to understand the core components of cybersecurity risk. Asking five questions can provide a critical first step in placing the cybersecurity risks a company faces in the right context. These questions — and the answers to them — inform the six principles that help executives and directors guide their organizations to a more mature and resilient program for managing cybersecurity risk. Answering these five questions can help firms reduce the impact of their next major security incident.

QUESTION 1: What is the organizational structure for oversight of cybersecurity risk management?

Mounting a credible challenge on cybersecurity risk requires an understanding of how the cybersecurity organization is structured, who holds key roles within it, and the position of those individuals within the larger company. Directors and executives should pursue a top-down approach and communicate frequently to engage cybersecurity and technology management.

Top-down in this context means, for example, board meetings to which management is invited, but at which it does not drive the agenda. A cybersecurity risk review should occur at least quarterly to...
keep abreast of changing risks and risk appetite. Board members should expect information and analysis on the organization’s cybersecurity risk management posture and any matters, regulatory or otherwise, requiring their attention.

Board members should be able to ask probing questions that help them determine what management is doing to address risks, and that degree of engagement requires their review of all relevant materials prior to meeting. That will help board members avoid questions that are not specific enough (Were you aware of this vulnerability?) or that invite a technical response that is too detailed (How did you close this technical weakness?).

Questions that can provoke important discussions include “What risks have you been most effective in reducing?” and “In what areas is it most difficult to mitigate risk?”

Be mindful of the skills and business acumen of the senior cybersecurity staff, particularly with a view to adding support where necessary. Even a seasoned chief information security officer may take some time to grow into the new demands of board-level reporting responsibilities. Organizations with the most successful cybersecurity risk management programs tend to have CISOs that wield influence throughout the organization, have substantial executive management expertise, and have strong interpersonal skills; being a competent technologist isn’t enough to guarantee a successful program.

Indeed, the right staffing is a priority throughout the cybersecurity risk management program as it becomes an increasingly important part of operational risk management. Organizations should emphasize finding cybersecurity professionals with experience in strategy, governance, and operations.

Additional questions on structure and resources that board members should ask and executives should be able to answer:

- Does the organization have a CISO? If not, why? Does the CISO have the right combination of skills to perform the role?
- Does the organization have adequate resources?
- How does the organization’s IT budget match up to its peers?
- Has the organization selected a cybersecurity risk management framework?
QUESTION 2:
How effective is the organization’s cybersecurity risk governance framework?

The right framework is risk-based, threat-informed, and tailored to the organization’s specific business requirements. Mature, sophisticated organizations rely upon a maturity-based framework such as the one put forth by the National Institute of Standards and Technology. Less mature organizations frequently fall back on a checklist-based approach.

A cohesive approach to the three lines of defense is also important. Information security policy oversight should reside in the second line of defense, but too frequently it sits in the first line with the IT operator — resulting in a conflict of interest, or at least a lack of checks and balances. Directors and executives should have a clear sense of how the first and second lines are divided.

The role of the CISO is not to always say no, but to help business lines — the first line of defense — mitigate risk through expertise and enterprise services. Through reporting, directors gain a better understanding of who owns cybersecurity risks, and whether they face the worst-case scenario: The first line doesn’t own the risk, and risk management — the second line of defense — isn’t adequately monitoring or reporting it.

Increasingly, public exposure is the ultimate arbiter in determining whether an organization has made the appropriate investments in measuring cybersecurity risk and setting its risk appetite to manage the risks.

Related questions:

- Has management set a cybersecurity risk appetite? If not, why? If yes, is it frequently reviewed and updated to adapt to the changing threat environment?
- Is the cybersecurity risk appetite reviewed by the board?
QUESTION 3: How is cybersecurity risk measured and reported to executives and directors?

Cybersecurity risk and impact should be incorporated in board reporting and addressed through metrics; ideally, through a dashboard that captures business impact.

It’s important to be able to have a dialogue with the organization’s top technology, cybersecurity, and risk leaders, who should be able to describe specific examples of meaningful metrics. A key element of this discussion is how the dashboard functions, and particularly whether it communicates business impact. That helps directors understand why a risk exists, as well as understand what must be done to reduce it. Dashboards that are a wall of numbers must be connected to the business to be of use. In the absence of crisp analysis, numbers don’t speak for themselves.

Related questions:

- When was the last time you received a cyberthreat brief?
- How do executives learn of significant cybersecurity incidents?
- How does the organization conduct benchmarking and how does it compare to peers?
- Is the business line accountable for responding to cybersecurity risks?

QUESTION 4: How is the organization managing risks related to the Internet ecosystem?

The mesh of interconnected information systems is the Internet ecosystem, and the risks within that ecosystem are shared by every connected entity in it. Weak cybersecurity risk management at a third party, outsourcer, vendor, or link in a supply chain puts every company within the ecosystem at increased risk.

Organizations try to address third-party risks through contractual requirements and vendor risk management programs. However, the further data and access control drift away from the organization’s own governance, oversight, and cybersecurity risk management framework, the harder it is to find and stop cybersecurity risk.
Organizations with relatively strong cybersecurity risk management have repeatedly been compromised by third-party errors — from unencrypted backup tapes falling off a truck to HVAC vendors with weak passwords. Poor risk management practices by vendors make organizations vulnerable.

Directors should incorporate third-party risk into their credible challenge. Organizations that rely heavily on outsourcing are at risk of becoming complacent and over-reliant — in which case it may only be a matter of time until a vendor shortcoming threatens the organization’s reputation and prompts a reassessment of its appetite for third-party risk.

Related questions:

- Does the organization have a risk-appetite statement for third parties?
- Does procurement assess a potential vendor’s cybersecurity procedures in bid selection?
- Do contracts with third parties include enforceable provisions related to their cybersecurity posture?

QUESTION 5:
What is the organization’s crisis-management strategy?

As the number of cybersecurity incidents mount and the threats continue to increase, organizations that once considered themselves low-probability targets are starting to reconsider that assessment. Pursuing new markets can mean attracting the attention of new adversaries and competitors. Changing geopolitical tensions may draw the interest of nation-states or foreign corporations. The lines between corporate intelligence, business competition, and hacking for IP theft continue to blur, especially for organizations operating in numerous jurisdictions. Sophisticated cybersecurity risk management executives know an incident is a matter of when, not if.

Organizations that traditionally have not seen themselves as likely targets frequently are at a disadvantage to organizations that have hardened their defenses over the years. Executives should incorporate incident response in their crisis management, public affairs, and outreach planning, and keep directors informed of the overall strategy. Devising a plan in the middle of a crisis perpetuates ineffective strategy.

A healthy paranoia serves organizations well, and those less prepared have suffered the consequences. A cybersecurity incident threatens more than just an organization’s reputation, and most of the damage that happens during a breach can be mitigated through early detection, containment, and mitigation. How you respond is just as important as how you build your defenses.
Six Principles for Cybersecurity Risk Management and Governance

1. Cybersecurity risk culture begins with the tone from the top. It demands engaged directors, executives, employees, and vendors.

2. Establish a cybersecurity risk-appetite statement. Leaders must insist on having a thorough understanding of the cybersecurity posture and a process for managing it just as other risks are managed.

3. Organizations must appreciate the nature of cyberthreats. Adversaries become increasingly sophisticated, and an organization’s response must match that sophistication. Threats include nation-states, industrial espionage, organized crime groups, and political hackers.

4. Cybersecurity risk reporting must be taken seriously. Information security is not built on compliance alone and must be constantly challenged to stay ahead of the curve. Benchmarking against minimum security frameworks and peers is important.

5. Organizations must take an unbiased look at their resources. In many cases, an organization’s infrastructure, third-party engagement, culture of trust, monitoring, and organizational structure must change to better integrate information security.

6. Expect a breach and work backward. A cybersecurity breach is a matter of when, not if. Developing a strong response capability is essential.
Related questions:

- Do executives have media-relations strategies and business-continuity and disaster-recovery plans? Have they gamed incident response, and conducted table-top exercises and fire drills?

- Does the organization have hunt teams actively looking for evidence of compromise?

Conclusion

Directors and top-line executives can do a great deal of good by asking the right questions about cybersecurity risk management and governance. Directors should demand clear, accessible disclosure — not data buried in an appendix to a huge report — and make sure they understand interconnections to third parties such as outsourcers and suppliers. Executives who prepare for these types of questions by taking the right steps on crisis management and planning will be able to pass the credible challenge that directors are mounting on cybersecurity risk management.
Contact Promontory

For more information, please call or email your usual Promontory contact or:

**Earl Crane**  
Director, Washington, DC  
e crane@promontory.com  
+1 202 370 0457

**Mike Joseph**  
Managing Director, Washington, DC  
m joseph@promontory.com  
+1 202 384 1013

**Gary Owen**  
Managing Director, New York  
g owen@promontory.com  
+1 212 365 6565

**Tim Roberts**  
Managing Director, London  
t roberts@promontory.com  
+44 207 997 3460

To subscribe to Promontory's publications, please visit [promontory.com/subscribe.aspx](http://promontory.com/subscribe.aspx)  
Follow Promontory on Twitter [@PromontoryFG](http://twitter.com/@PromontoryFG)