Cyber Risk and Resilience for Boards

Cyber risk and resilience for boards

Cyber risk is one of the top 10 global business risks[1]. Like all other enterprise risk, it threatens the ability of an enterprise to succeed in its business strategies. Certainly, an impaired information infrastructure affects the ability to conduct business. Any risk that threatens the ability of an enterprise to perform business transactions must be a board focus.

[1] Forbes/AON global risk management report

Contents

Your role in cyber risk and resilience

Among your primary responsibilities as a board member is providing advice on both business strategy and enterprise risk.

A general understanding of risk management is essential when looking at cyber risk specifically. Ultimately, an enterprise should consider adding cybersecurity expertise to its board membership, but all members can benefit from increasing their understanding about how cyber risk affects corporate strategy and the overall enterprise risk profile.

To provide effective strategic advice to company leadership on cyber risk, you must ask the right questions, including **whether** a company does ongoing cyber risk assessment and management, and **how**.

Step 1: Understand your tolerance for risk

Awareness of the risks that your enterprise faces is not enough. You also have to understand how willing you are to accept risk in general and whether certain risks are easier to bear than others. For example, most enterprises are unwilling to risk harm or death to people. However, the same enterprise that cannot accept risk to human safety might be comfortable with a heavy risk from investing in scientific research that might produce nothing of commercial value.

To gauge your tolerance or “appetite” for risk, first consider your organization’s current risk management activity.

If your enterprise does not have a current, active set of management activities to identify, prioritize, and mitigate risks, then the board can do nothing further until the enterprise solves this problem. Risks constantly change. If your enterprise is ignoring risk, that may be the most serious risk and the first problem to address.

Ask the senior leaders a few basic questions: What are the top risks faced by the enterprise? How often is that list reviewed?

- Does a current, prioritized list of risks exist? Priorities must reflect the impact of a risk, potential rewards (reasons to take the risk), and what the company can do to mitigate each risk
- Which staff teams are responsible for managing and mitigating those risks? How often are these processes reviewed?
- What residual risk remains after mitigation? How often is residual risk reviewed?

You can ask the same questions about cyber risk without having specific expertise, because these questions focus on whether anyone in the enterprise is working on risk as a problem.

Consider a worst-case exercise: Can your enterprise bear the burden if any or all risks are triggered and the company must pay the residual risk impact that it estimated?

- If the enterprise faces five major risks with a residual risk exposure of $2 million each, the total exposure to residual risk is $10 million. Does the company have the cash on hand to cover this exposure if all five risks are triggered at once?
- Reputational risk is also an issue. Is the company willing and able to accept damage to the brand if a risk is triggered? For example, what if customers stop buying for a month? What if they stop for 3 months?
- Can the enterprise continue operations if the risk is triggered? What if the enterprise buys from a single vendor? Maybe it buys from three vendors, but all three are in the same city, and that city is on a fault line, in a war zone, or in a politically volatile nation—some circumstance that might make all three vendors unavailable at the same time

Step 2: Build a risk-tolerance profile

Determining answers to all these questions can help you build a risk tolerance profile for an enterprise—one of your most important tools when advising the enterprise. For example, an enterprise with very little tolerance for risk associated with exchange-rate volatility in a specific nation is unlikely to ever consider business opportunities in that nation, regardless of other factors that favor those opportunities. It would be a waste of time for both the board and the enterprise to discuss those opportunities until the issue of sensitivity to exchange-rate volatility changes.

By focusing your questions specifically on cyber risk, you can arrive at a profile for cyber risk tolerance. Consider an enterprise that stores and protects backups of U.S. Department of Defense computer systems. The enterprise clearly has a high tolerance for risk associated with the possession of classified information. If the enterprise is seeking new business opportunities, the board might suggest, for example, that it consider offering offsite storage of sensitive backups to the legal community. Law offices often have large amounts of very sensitive information about their clients and little ability to protect it because data protection is not core to their business, although it is essential that they handle the data properly. They are typically aware of the financial, reputational, and operational risks of possessing that client data and might be willing to transfer that risk to a company better able to deal with it.

Cyber risk is only one example of a critical risk category for enterprises. The board can create a specific risktolerance profile for any common enterprise risk. The process for building a cyber risk profile is the same for building a general risk profile, and the questions will be similar. The goal is to determine whether the executive team is actively managing cyber risk. The resulting profile guides the board in advising the enterprise on cyber governance, strategy, and risk management.

Step 3: Encourage effective cyber resilience

Cyber resilience comprises the information services and technologies that ensure the stability, availability, confidentiality, and integrity of the enterprise information infrastructure. Cybersecurity services, backups, performance planning, incident response, compliance and audits, business continuity plans, security awareness, and similar activities are all part of enterprise cyber resilience. Your enterprise already does cyber resilience to some extent. The suggestion here is to govern these services within a specific cyber resilience program and to require senior leadership accountability. The goal is to reduce the risk and costs of infrastructure outage by improving the structure and function of cyber resilience services and technology.

Cybersecurity is often a mystery to boards. The entire board does not need a deep technical understanding, although broad knowledge of cyber risk is helpful. Boards typically have experience in dealing with risk—even risk from highly technical disciplines about which members might not have deep understanding. However, experts in high-risk technical disciplines are not always able to communicate effectively to business leaders. Consider requiring experts to meet the board halfway with communication. It is possible to discuss cyber risk in plain English, and in financial terms, without using technical jargon. The ability to speak clearly about cyber risk is a useful skill for security technologists to develop.

To encourage effective cyber resilience, focus your questions on three broad topics:

- **Technology:** Given the risk profile for the enterprise, is the right set of technologies and services in place to ensure the appropriate levels of confidentiality, availability, and integrity of the information infrastructure for the enterprise?
- **Culture:** Does the enterprise have a culture of continuous improvement for information services, including all of the cyber resilience services?
- **Metrics:** Does the enterprise use the right resilience metrics and regularly review them? Are less useful metrics identified and eliminated and new metrics added over time?

Specific questions to ask of the enterprise leaders include:

- How do you mitigate the top risks defined in the cyber risk profile?
- Is the budget authority for cyber resilience at the right level?
- How do you measure performance of the security and resilience functions?
- Are core business and financial processes adequately secure? What is the evidence?
- Do you adequately secure regulated data and corporate information? What is the evidence?
- If you were hacked, how would you discover it and when? What is the plan for handling breaches?
- What methodology do you use to continuously improve cyber resilience services and technologies?
- How do you test cybersecurity and resilience functions? How do you use the test results?

Your enterprise can use the cyber risk profile as a guide for indirectly defining the security budget. The risk profile defines negative events, how much damage will occur when negative events happen, and how to minimize the chances of occurrence and damage. Developing mitigations for cyber risks can lead to a budget number for addressing those risks.

The IT industry, compliance and legal environments, and cybercrime are all changing. As enterprises evolve, the services and technologies that addressed yesterday's risks might no longer be valid. Even if they are, improvements can reduce costs and boost performance. With a culture of continuous service improvement, enterprises can deliver updated services that are less expensive and more useful.

> **"Measurement is the first step that leads to control and eventually to improvement. If you can't measure something, you can't understand it. If you can't understand it, you can't control it. If you can't control it, you can't improve it."**
>
> **– H. James Harrington**

Measuring cyber resilience effectiveness

Measuring the effectiveness of cybersecurity services is one of the most challenging goals for the cybersecurity industry. Therefore, the board should regularly ask, Do our measurements tell us whether we are meeting our objectives for managing cyber risk? How?

Consider the problem of phishing, which often specifically targets boards of directors. Phishing is a high-profile attack tool that can bypass an enterprise's technological defenses.

It's not hard to find information about phishing. Just search the Internet for "phishing" and "best practices"[1, 2, 3] or "defense."[4, 5] How do you measure your ability to defend against phishing? By the number of people who pass a phishing awareness class? By how many people click on links in phishing emails?

Some companies take a proactive approach to this problem:

- Employees are required to pass a class in phishing awareness each year.
- A small security operations team stays current on phishing techniques and constructs tempting phishing messages that test company employees. Phishes might be general scams, spear phishes against specific groups or people, or "whale phishes" that specifically target senior leaders and board members.
- Alert recipients will detect suspicious intent and forward the suspect email to the security operations team.
- Recipients who are lured into clicking the link are taken to a security operations page where they can learn how they were fooled and what to do in the future.
- By analyzing phishing activity, security operations teams can determine the following:
- Which techniques work best (an opportunity to train people)
- Who is most susceptible (another opportunity to train people)
- Overall success rate for the security operations phishing test
- Quantity of captured hostile phishes per unit of time (attack intensity against the enterprise)
- Obvious trends such as whether employees are becoming better at defending themselves

You can use this data to determine the return on investment for phishing awareness campaigns. For example, if the average breach costs around $3.8 million to remediate,[6] and the trend is fewer successful phishes over time, then the company is saving $3.8 million for each reduction in the average number of successful phishes over time.

Proactive security awareness programs lead to positive, measurable outcomes:

- Security operations has a regular means to assess vulnerability within the enterprise
- Data measures the practical effectiveness of security and guides meaningful improvement
- Employees gain security awareness
- Security operations can learn what works and what does not
- Measurable outcomes can be expressed in financial terms

[1] https://www.sophos.com/en-us/security-news-trends/best-practices/phishing.aspx

[2] http://www.globallearningsystems.com/blog/post/10-best-practices-to-avoid-email-phishing-attacks/

[3] http://www.globallearningsystems.com/blog/post/10-best-practices-to-avoid-email-phishing-attacks/

[4] http://www.networkworld.com/article/2161950/infrastructure-management/best-practices-to-close-the-door-to-spear-phishing-attacks.html

[5] https://digitalguardian.com/blog/phishing-attack-prevention-how-identify-avoid-phishing-scams

[6] http://www-03.ibm.com/security/data-breach/

Conclusion

Boards already have experience in risk analysis and in asking questions that guide executive leadership. Cyber risk is not inherently different from other enterprise risk. Obstacles are technical complexity and a lack of standardized language for expressing cyber risk in financial terms, but there are ways to overcome these obstacles. For example, Cisco offers regular briefings and tours that demonstrate how we approach cyber resilience.

You can manage and improve cyber resilience and cybersecurity by applying any structured methodology for service development and continuous improvement, such as that offered by the Information Technology Infrastructure Library (ITIL), the ISO 20000 global standard for IT service management, or DevOps. Your enterprise might be able to add service management expertise to the cyber resilient staff.

Questions that a board asks about any enterprise activity apply to cyber resilience. However, board members should be aware that the ability of cyber resilience teams to determine and measure effectiveness is often minimal. This is common throughout the cybersecurity industry. Therefore, consistent board pressure asking for evidence of ongoing cyber risk planning and mitigation is critical.

C11-739551-00 08/17