Closing the Cybersecurity Knowledge Gap in the Boardroom

Overview

Many boards have a significant knowledge gap on cyber risk and security. Chief Information Security Officers (CISOs) can bridge that gap by advising board members on this important topic in business terms they readily understand. This paper provides four steps CISOs can take to help boards and business leaders determine the business risk of cyber threats, prioritize security investments, and measure improvement in security performance. Doing this gives CISOs more influence in the boardroom so they can help ensure their organizations are protecting critical assets, privacy, and their reputations while safely driving critical business strategies.

In a recent study commissioned by Cisco, board members and business leaders from Global 2000 companies revealed that only one-third of boards have the level of knowledge they need to effectively govern cyber risk. These research participants span nine industries in 12 countries.

Why does this knowledge gap matter? Cyber risk is one of the top ten global business risks. (Source: Forbes/AON Global Risk Management Report). Like all other enterprise risks, it threatens the ability of an enterprise to succeed in a dynamic environment.

"Most boards that I've worked with don't even understand the true definition of cybersecurity."

– COO,
Fortune 1000 Retail

Contents

If boards don't understand cybersecurity, how can they govern cyber risk as their business changes? Across industries, one of the major business changes is digital transformation. Digital transformation uses technology to build new business models, processes, software, and systems that create a competitive advantage by helping to increase efficiency, revenue, and margins. Businesses achieve this by transforming their approach to capturing value, creating new customer experiences, and keeping security a priority. Think about Uber, Airbnb, and Square, and how they have revolutionized transportation, accommodations, and purchase transactions, respectively.

Yet, while a majority of business leaders agree that cybersecurity is important to digital transformation, most lack a formal strategy to put it in place. According to the study:

- 80 percent consider digital transformation a strategic priority and formally plan for it.
- Only 50 percent of organizations plan for cybersecurity before initiating digital transformation.

As digitization of business moves forward, the potential for exposure increases as more devices are connected and critical processes take place online. Adversaries have more tools at their disposal than ever before. The explosive growth of mobile endpoints, new Internet of Things (IoT) devices, and online traffic provides them with more space to operate, and more choices in terms of targets and approaches.

Without upfront security plans, many organizations remain vulnerable, not only to breaches, but to losing their competitive edge if they can't innovate quickly.

- 71 percent of executives said concerns over cybersecurity are impeding innovation in their organizations.
- 39 percent stated they had halted mission-critical initiatives due to cybersecurity issues.

Developing an effective security strategy is essential to protecting current business operations and innovating quickly to gain a competitive advantage. One way forward is to give security leaders a voice earlier in the development of strategic initiatives and risk management plans. This helps them build a cybersecurity strategy into plans up front, and leads to less complexity and fewer halted initiatives. The bottom line: security can help a business succeed rather than present a roadblock.

"It used to be that line-of-business leaders looked at the security folks as roadblocks. I think they're starting to understand now that they're there to help them be successful."

– Board Member, Global 2000 Energy

How security professionals can help close the gap

Chief Information Security Officers (CISOs) know the intricacies of their businesses better than outside experts, but often are not consulted for strategic guidance. Including CISOs in risk management discussions and empowering them to effectively communicate can give security leaders a strategic voice in long-term planning. The study revealed that:

- Only one-third of boards and executives rely primarily on the CISO for education on security issues.
- CISOs are often perceived as too technical, leading boards to seek security guidance from external sources.
- CISOs are excluded from business strategy conversations because cybersecurity planning is often done after the fact rather than integrated into the plan.

It does not have to be this way. With the escalation of cybercrime, the role of a CISO is fast evolving beyond its traditional operational functions of monitoring, resisting, and responding to cyber threats. Continuous changes in the connected business landscape make customer data, intellectual property, and brand properties new targets for information theft, which can directly impact business performance and shareholder value. In response, CISOs are progressing to a stronger leadership role, with an imperative to move beyond the confines of reaction and enforcement.

If you are a CISO or IT leader looking to take a stronger leadership role, there are several actions you can take to boost your effectiveness when you meet with your board and senior executives. In addition to sharing current trends in cyberwarfare and current threats, you can provide more strategic advice. To do so, it's best to focus on the following four areas:

- Understand the board's appetite for risk and get involved in the enterprise risk management (ERM) function.
- Build a risk profile aligned to enterprise risks.
- Measure risk and set effectiveness metrics.
- Demonstrate effective resilience and continuous improvement.

Taking this approach will help you effect change and get the support you need for high priority security projects. It will also get you a seat at the table.

Step 1 – Understand your board's appetite for risk

As Steven Covey says in **Seven Habits of Highly Effective People**, "Seek first to understand, then to be understood." Start by understanding the risk management philosophy, goals, policies, and enterprise-risk-management function at your company. If you don't have an understanding of business risk management, that's a problem you need to solve. IT security exists to mitigate business risk associated with the use of technology and computer systems.

The ability to speak about risk in business terms is the skill necessary to sit at the table with enterprise leaders. In order to be accepted, CISOs need to:

- Understand the goals, philosophy, and policy of the business with regard to risk and risk management.
- Demonstrate knowledge of the digital assets and business processes, including ownership, importance, business risks, and current mitigations.
- Take part in the enterprise and IT security risk management functions, and know all of the stakeholders.
- Actively engage senior leaders in discussion of how cybersecurity can support existing business activity and spur new business initiatives.

With this groundwork accomplished, senior leaders and the board can accept the CISO as an insider and a team player, someone who has a voice in their discussions.

Step 2 – Build a risk profile aligned to enterprise risks

Once you understand the board's appetite for risk, the next step is to build a cybersecurity risk profile tied to the Enterprise Risk Management (ERM) process. This is important because boards are responsible for governing risks such as intellectual property, reputation, legal or regulatory compliance, and monetary vulnerabilities. A risk profile informs them about cybersecurity risk in terms they understand. Put simply, a risk profile is an evaluation of an organization's willingness to take risks as well as the threats to which an organization is exposed. It's important for determining the proper level of effort and investment needed to secure a company's assets.

You should not develop this profile in a vacuum. Do it in collaboration with wide variety of stakeholders within the organization, including business leaders, data and process owners, enterprise risk management, internal and external audit, legal, compliance, privacy, and the Information Risk Management Security (IRMS) team.[1] This risk profile, if created correctly, will tie easily into the ERM process. This process identifies mitigations for reducing enterprise risk sorted by magnitude of business impact. Keep in mind: details regarding a breach or mitigation may be technical, but the risks are not. With IT security, the risks lie in three areas:

- IT infrastructure, including hardware, software, applications, and IOT devices.
- Connections to partners, vendors, and customers
- People's actions and awareness when interacting with systems.

To develop an effective risk profile, you first need to understand what impacts would matter most to the business and what threats could result from these impacts.

Example 1: A manufacturer needs its production lines running in order to conduct business. The organization would have a low tolerance for risk from threats to the operational integrity of their production lines and ancillary systems.

Example 2: A healthcare facility requires that its patient monitoring systems, infusion systems (medication pumps, dialysis systems, and others), and patient records be continuously available to reduce the potential loss of life. The facility has an extremely low tolerance for risk created by the lack of availability of those systems. For the most part, healthcare facilities have traditionally mitigated this risk by helping to ensure they have protections such as back-up power using generators. Now they also have to consider threats such as Denial of Service (DoS) or ransomware attacks.

Cyber threats are continuously changing and increasing in severity. Many organizations have a poor understanding of how fast the threat landscape can change and may lack processes for quickly taking preventive action. For example, Windows Management Instrumentation (WMI) was believed to be low risk until it was used to help enable WannaCry ransomware to spread. This type of cyber attack encrypts data until the user pays. The Nyetya (or Not Petya) attack was malware hidden in a vendor's software updates that delivered a destructive payload disguised as ransomware. Both of these attacks spread quickly to multiple businesses and dramatically affected operations. Attacks targeted at a specific company can have just as severe an impact. Millions of consumers are at risk because of a large financial institution's failure to patch a well-publicized software vulnerability, quickly detect the breach, and recognize the severity. As a result, the company faces lawsuits and congressional scrutiny, and several of the company's leaders have left the company.

1 https://www.isaca.org/Journal/archives/2013/Volume-4/Pages/Key-Elements-of-an-Information-Risk-Profile

"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

Step 3 - Measure cyber risk and establish real metrics

Measurement is crucial to understanding real risk and being able to show and talk about continuous improvement. The goal is to create metrics that measure risk and cyber resilience. Step 3 includes a discussion of cyber threats and controls necessary to prevent, slow, detect, and respond. It's important to remember that many of the day-to-day security activities will result in technical metrics that directly help security and IT management understand exposure and control effectiveness. However, these metrics are not appropriate at the board level. Step 4 provides an example of a high-level metrics dashboard that you can share with the board and senior business leaders.

Since cybersecurity is often a mystery to boards, you'll want to discuss cyber risk and resilience with them in business or financial terms, without using technical jargon. With this in mind, clear definitions are important to establish proper risk definitions:

- **Vulnerabilities**: weaknesses that exist in the network infrastructure, IoT devices, software, or supporting processes.
- **Threats**: negative events that would exploit vulnerabilities and lead to undesired outcomes.
- **Risk**: the chance of negative impact multiplied by the likelihood of occurrence.

With the definitions clearly established, it's best to avoid discussing vulnerabilities at the board level, but the metrics around them will play into the higher-level conversations regarding potential threats and risk levels. The difference between a threat and a risk is a common point of confusion. While a threat is a negative event in itself, a risk is the likelihood and impact of a negative event.

Once you understand the vulnerabilities, threats, and ultimately, the risks, what are the real metrics that are going to demonstrate the level of risk and the effectiveness of controls? When approaching the board, you won't directly present these metrics but, rather, the story that the metrics tell you. Essentially, you will be tracking two types of metrics: internal metrics that assist in determining trending and effectiveness and the result of that analysis, which you present to the board.

Internal metrics may include:

Infrastructure statistics

- Number of critical and high-risk vulnerabilities
- Number of critical and high-risk vulnerabilities remediated
- Number of vulnerabilities by type
- Number of patches applied; number of critical security patches applied

Program statistics

- Number and types of assessments or audits performed
- Number and type of policy changes made
- Security awareness and training performed; number of staff trained

Board metrics may include:

Risk statistics

- Increase or decrease in industry threats
- Increase or decrease in types of threats (network, cloud, mobile, IoT device, OS, application, and others)
- Increase or decrease in policy exception
- Increase or decrease in security staffing or budget

Threat mitigation statistics

- Time to detect, time to contain, time to patch, time to remediate
- Length of system outages due to breach
- Percentage of systems impacted due to breach
- Type and number of systems affected (network, cloud, mobile, IoT device, OS, application, and more)

Keep in mind, effective metrics:

- Are simple
- Drive decisions and actions
- Can be base-lined
- Trend over time
- Define what a good outcome looks like

Step 4 – Demonstrate effective cyber resilience and continuous improvement

Assuming you are effectively measuring security and risk, you will want to demonstrate effective cyber resilience and continuous improvement to the board. Cyber resilience comprises the information services and technologies that help ensure the stability, availability, confidentiality, and integrity of the enterprise information infrastructure. Enterprise cyber resilience includes:

- Cybersecurity services
- Backups
- Performance planning
- Incident response
- Compliance and audit
- Business continuity plans
- Security awareness
- Similar activities

Effective cyber resilience helps reduce risk and costs of infrastructure outage by improving the structure and function of cyber resilience services and technology. Are you likely to reduce risk to zero? No. Not only because being 100 percent secure is impossible, but even if that were not the case, it would be cost prohibitive. The goal here is to secure things to a level of effort and budget in line with the risk or exposure to the company. It's important to help your board members understand this, as they must be reminded that nothing is foolproof. It also does not help to suggest that all is well. The assurance that everything is perfectly protected and without risk would likely result in skepticism from the board rather than confidence.

To communicate effectively with your board, focus your discussion on four broad topics:

- **Technology:** Given the risk profile for the enterprise, recommend technologies and services that help ensure appropriate levels of confidentiality, availability, and integrity of the information infrastructure.
- **Culture:** Explain your culture of continuous improvement for cyber resilience services.
- **Metrics:** Regularly review resilience metrics. Identify and eliminate less useful metrics and add new metrics over time.
- **Audience:** Operational security metrics mean nothing to board members, but they will recognize improvement over time. They will also be very interested to hear about any return on investment (ROI) on security expenditures. In addition, help them understand that, as the security program makes strides, the business will be able to move forward with new initiatives more easily.

Show how results reported from security operations are fed into the risk management function, and how the risk management group reacts to this input by modifying business impact, approved mitigations, and approved funding for mitigations. These metrics show risk management as iteratively improving and responding to a dynamic risk environment.

Finally, when discussing how effective your cyber resilience program is, use an easy-to-understand dashboard such as the one in Figure 1. Effective dashboards:

- Are easily consumed
- Provide messaging
- Combine data and commentary
- May summarize metrics
- Answer essential questions

Figure 1. Effective Dashboard Example

Cyber Security - Overall Program

Mission Statement

Cyber Security & Risk Management provides services to maintain the confidentiality, availability, integrity and accountability of information technology systems and operations through secure engineering and risk management.

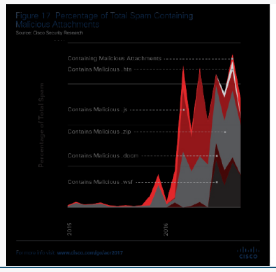
Key Risk Indicators	Level	Trend	Key Performance Indicators	Level	Trend
Cyber security incidents		▲	Cyber security budget		–
Critical infrastructure incidents		▼	Cyber security staffing		▲
Industry threats		▲	Cyber security plan progress		–
Policy exceptions		▲	Industry threats blocked		–

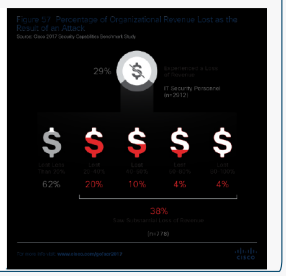
Summary of Changes to Risks and Mitigations

Risks:
- Increasing industry threat indicators reflect ongoing trend
- Ransomware and phishing attempts increased in quarter
- Increased use of third party cloud applications
- Personnel and skill set shortages

Mitigations:
- Optimizing roles and cyber security org structure
- Accelerating hiring - 3 offers /2 accepts in last 30 days
- Enhancing career development and training
- Improving incident response processes

Spotlight: Industry Threat Trends





Effective cybersecurity dashboards include the following:

- Risk and performance indicators
- Mitigation plan for the top risks defined in the cyber risk profile
- Industry threat trends
- Security technology and risk program performance
- Security of core business, financial processes, regulated data, and corporate information
- Financial implications

The IT industry, compliance and legal environments, and cybercrime are all changing. As these business influencers and your business model evolves, the services and technologies that addressed yesterday's risks may no longer be valid today. Even if they are, improvements can reduce costs and improve performance. With a culture of continuous service improvement, your organization can deliver less expensive, more useful updated services.

Conclusion

Boards already have experience in risk analysis through asking questions that guide executive leadership. Cyber risk isn't inherently different from other enterprise risk. CISOs can help boards build a cyber risk profile that helps their organizations focus on protecting the enterprise's most critical assets.

As a CISO, you can have a business-focused, forward-looking conversation with your board and business leaders, one that demonstrates how essential an effective cybersecurity strategy is for digital transformation. You can provide:

- Recommendations on how to best protect the organization's most critical assets in alignment with the enterprise's cyber risk profile.
- Meaningful metrics to help leaders understand the progress the security organization is making.
- A plan to rapidly respond to cyber attacks.

This kind of conversation can transcend fatigue, provoke real, long-term change, and create a new perspective. Giving cybersecurity a strategic voice not only protects customers and revenue, but also lifts up the whole organization as a leader in its industry and segment.

Are you interested in leading board discussions about business risks or the financial impacts of cyber risks? Are you interested in learning more about developing the right security metrics and dashboard for your business? Would you like to supplement your security organization with incident response management services? Are you embarking on a secure digital transformation project? Cisco Security Services can help provide the expertise and supplemental resources you need to you achieve these important strategic goals.

Why Cisco?

Our services and solutions are delivered by highly trained, experienced security experts who are focused on your business and understand your challenges and objectives. Cisco Security Advisory Services can help you understand the risk profile of your organization, and whether it aligns to your risk tolerance. We assess risks internal to your operations, as well as those from third parties, and help you learn how to manage rigorous compliance requirements. With this knowledge, you can make more effective risk decisions about how you connect, communicate, and collaborate.

More Information

To learn more about Cisco Security Services, visit cisco.com/go/securityservices.

[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/

C11-739745-00 11/17