PONDURANCE

5 Best Practices for Reporting to Your Board About Cybersecurity

INTRODUCTION

Reporting to the board of directors may be intimidating for many chief information security officers (CISO) and chief information officers (CIO), but it's also a huge opportunity to demonstrate leadership, increase understanding of current and future risks and make a persuasive case for additional budget or other resources. Ideally, your reporting will even enlist board members' participation in efforts to reduce your company's risk profile, such as implementing stronger security policies and supporting a culture of cyber hygiene.

To accomplish your goals, you need to prepare carefully and rigorously for each session with the board. It's critical to understand what types of information your board members are looking for, how to present it effectively in a limited window of time and which pitfalls to avoid, such as using cyber jargon and diving too far into technical details. This whitepaper offers practical guidance to help you report to your board about cybersecurity successfully. Following these leading practices can enable you to expand board members' understanding of information security, win their support for your objectives and burnish your professional standing in their eyes.

DUE DILIGENCE: Preparing for your presentation

You should expect to meet with your security and risk committee each quarter for a detailed discussion of your security program. The goal of this meeting is to identify important and relevant information, such as trends, current threats and metrics, and summarize it in a concise dashboard for presentation to the full board.

During the security and risk committee meeting, you should query the members about their recommendations for the format of the dashboard and the types of data it should contain. See a list below for examples of information to consider for inclusion in the dashboard. Your list of categories should be adjusted to reflect the board's interests and concerns.

5 BEST PRACTICES FOR BOARD PRESENTATIONS

1. **Research board members' areas of focus and levels of security knowledge**
2. **Deliver a concise and business-oriented presentation**
3. **Address strategic security questions each time to show trends and progress**
4. **Cite select key performance indicators (KPIs) and illustrate with examples**
5. **Prepare a detailed appendix to back up metrics**

INFORMATION TO CONSIDER FOR YOUR DASHBOARD

- **Intrusion attempts:** The number of times malicious actors tried to gain unauthorized access to systems, networks and software
- **Mean time to detect:** The time it took to detect security threats
- **Mean time to resolve:** The time required to respond to a cyberattack
- **Mean time to contain:** How long it took to resecure the attack location
- **Patching cadence:** How frequently you install security patches
- **Comparison with peers:** Your company's cybersecurity posture compared to that of industry peers
- **Vendor risk management:** How your company mitigates risk in the supply chain to prevent vendors and other third parties from causing a data breach

PONDURANCE

As part of preparation for your board presentation, make every effort to learn about the individual members and their areas of expertise, experience and concerns. This information will help you determine the best approach for demonstrating your successes, your ongoing challenges and your current and future strategy for mitigating risks and managing the overall security program.

LESS IS MORE

Typically, you'll have only 15-30 minutes to present, so limit your slides to a handful:

1. **Risks and events**
2. **Projects with status and budget**
3. **Implementation of controls**
4. **Findings from tests, audits, and exercises**
5. **Answers to strategic security questions**

Supplement the slides with a detailed appendix.

> **"Avoid reporting for reporting's sake. Generally speaking, there is greater risk in reporting too much data rather than too little."**
>
> - Corporate Board Member magazine[1]

IMPACT AND PROBABILITY: Presenting cyber risk to the board

The way you describe and quantify the cyber risks facing your company can make a big difference in board members' understanding. It's critical to choose metrics carefully and explain what each one means and why it matters to the organization.

Start by categorizing the types of risk that are most relevant to your company and industry and then explain the potential impacts of each type in terms that the directors are most familiar with, that is, business language.

- *Defining cyber risk by category*

Since cyber risk is not monolithic, it's important to ask the security and risk committee for feedback on which types are of greatest concern to the board. This group might wish to categorize risk by its impact on confidentiality, integrity, availability, utility, control, authenticity and privacy. Or it may prefer categories such as third-party risk, risk of a business interruption, risk of a data breach or a ransomware attack, risk of a regulatory fine, etc.

- *Expressing cyber risk in financial terms*

According to NIST SP 800-30, *"Risk is a function of the likelihood of a given threat-source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization."*

Cyber risk is a form of business risk that can be expressed in financial terms (revenue loss, mitigation costs, legal fees, increased customer turnover, reputational damage). Boards of directors can more easily grasp cyber risk when it is quantified using financial metrics rather than abstract rankings such as high-medium-low. In doing so, however, it is important to represent risk as two independent factors: impact and probability. Impact is always expressed in cost terms, while the probability of a given incident's occurrence is estimated or calculated (e.g., based on factors such as past experience, available threat intelligence, etc.).

You can graph impact and probability using a curve to show how, as the impact increases, the probability declines. Another way to visually convey risk is with a heat map, which uses colors (e.g., red, yellow, green) to indicate the relative significance of different risks to which your company is

exposed. However, a heat map can be problematic in that it obfuscates the fact that the probability of a very impactful event is always more than zero.

TIME AND MONEY: Reporting on current projects

Typically, board members will expect a report on projects your team is working on to prevent, detect and remediate cyber risks. They will want to know if these projects are proceeding on time and on budget and, if not, the reasons why. If the issue is a lack of resources or budget, the board may be willing to help. Be prepared to explain how you will use additional resources to expedite project completion. If you fought for funds at a prior board meeting, the members probably will request a status report on the use of this money and how it is helping to improve security.

Following are some tips on reporting to the board about your projects. First, be sure the report content is appropriate for the audience, which means supplying high-level objectives, costs, timelines and return on investment rather than a lot of technical details. Second, you need to reiterate the company's position on risk tolerance (risk appetite) and align it with your project's objectives. When board members understand and support your strategy for risk assessment and prioritization, it becomes easier to obtain their buy-in on your tactical activities. Finally, because cybersecurity projects are often driven first by regulatory requirements, be clear about what must be accomplished to ensure the business can achieve and maintain compliance.

UP TO STANDARDS: Reporting on implementation of controls

Another important metric for the board is the percentage of recommended or required controls you have implemented, which can be determined through cyber risk assessments. For example, you may report that you have implemented 85% of the preventive controls under the NIST Cybersecurity Framework at tier 1 and the remainder have been matured to tier 2. Questions from the board may include which controls have been matured to tier 2, why you prioritized these particular controls, and when the tier 1 controls are slated for migration to tier 2 (and when tier 2 controls will migrate to tier 3).

In general, details about individual controls are less important to board members than high-level control families, so it may be advisable to create an aggregate view of these families. You can show an overview of the status of controls by tier (identify, protect, detect, respond and recover) on your dashboard and indicate the percentage completed and percentage remaining at each level. To supplement this information, you may wish to create an appendix with details on both the elements within the controls and the particulars regarding tier levels and completeness.

In addition, the appendix should explain why you selected each control and whether it mitigates impact, probability, or both. If you have a way to measure risk reduction from these controls, the appendix is a good place to provide more information for board members who want a deeper dive.

HIGH/LOW MARKS: Reporting on audits, penetration tests and business continuity exercises

Findings from security audits and penetration tests should be presented to your board along with your plans for addressing those results, both positive and negative. Relay this information in business rather than technical terms but offer details in the appendix to your dashboard.

Types of information you could provide include:

- Point-in-time assessments, such as penetration test results or compliance audit findings, with a plan of action and milestones containing risk mitigation recommendations
- Progress against baseline assessments to show growth and maturity of the security program

Comparing audits and penetration tests to the ones performed in previous years is valuable but, if results are becoming worse, be prepared to explain how you intend to turn that trend around. You'll want to follow up at future board presentations with a status report on actions that are being taken to improve outcomes from audits and penetration tests.

Similarly, you should inform the board about any simulations of cyberattack response and business continuity exercises that you conducted since the previous meeting. As we've mentioned before, it's important to report on what went well and what went poorly, and your plans to address the latter. Put this information into the context of the business (e.g., how fast you could respond

to an attack or resume business operations after a breach and what that timeline would mean in financial terms).

IN THE HEADLINES: SHARING CYBERSECURITY NEWS

Because your board undoubtedly follows the news closely, you should explain how you are addressing high-profile cyber threats such as ransomware, credential theft, Internet of Things attacks, spear-phishing, supply chain weaknesses, or vulnerabilities such as Log4j that could affect your organization. Report on the threats and risks that are currently trending and whether your company is protected. This is a good opportunity to demonstrate your in-depth knowledge of different types of threats, the industry sectors they target and best practices for combating them.

TRACKING TRENDS: REVISITING STRATEGIC SECURITY QUESTIONS

Each time you present, go over the same brief list of high-level questions to show trends and indicate progress you are making to improve the organization's security posture. This exercise will provide continuity from one board meeting to the next. Following are suggested questions to answer:

- What is our current cyber risk level?
- What are our top security risks this quarter?
- Is our security posture improving or worsening?
- Is our security spending appropriate for our current risk level?
- What is on the horizon in terms of new threats and new risks?

SPECIAL BOARD PRESENTATIONS

Aside from regular, quarterly presentations to your board, you may be involved in special meetings in response to an incident or business change. Following is some guidance on how to handle these ad hoc board meetings.

The dreaded data breach meeting

As part of your procedures for breach and incident response, you should create a plan – both at the technical and board levels – to address lessons learned. The best time to do this is before an incident occurs.

Tabletop exercises conducted with the board are a great way to test the output of your lessons learned plan. This tactic shows your proactive stance and helps clarify how the members want to receive this information.

If a data breach occurs on your watch, you can expect aggressive questions from the board about what happened, the tactical and strategic implications for the business, how you are addressing the issue, and how you plan to avoid a recurrence.

To prepare for this detailed and possibly fraught interchange, thoroughly research and document the root cause of the breach. If the attack circumvented controls you previously implemented and reported on to the board, the directors will undoubtedly question why they were not effective in stopping the attack. If your prior reporting did not flag any issues with these measures, the questions may turn into accusations.

> **"Contrary to popular belief, data security begins with the Board of Directors, not the IT Department."**
>
> - U.S. Federal Trade Commission[2]

PONDURANCE

To understand the board's attitude, remember that directors may be liable if they fail to exercise care and diligence in relation to cybersecurity, including safeguarding the organization against financial costs, reputational damage and legal repercussions from an attack.

On the other hand, if the attack was not related to existing controls, you may be able to make a case for more resources to implement new technologies or processes.

The meeting about upcoming business changes

A well-run board will involve the CISO or CIO in advance when a merger, acquisition, new facility, new partnership or other major business change is in the works. The board will want you to research the project and report back on any associated cyber risks. For instance, in considering a potential acquisition or merger, they will seek reassurance that the entity did not experience and fail to properly report a previous data breach. In other words, they don't want surprises.

Marriott and Verizon both discovered the serious ramifications of such a surprise. When it acquired hotel properties from Starwood in 2016, Marriott was unaware of a "compromised database breached by bad actors who were duplicating, encrypting and working to erase personal data of guests," according to CIODive. The breach impacted 500 million hotel guests.

In Verizon's case, its 2017 acquisition of Yahoo! was put in jeopardy after breaches affecting 3 billion Yahoo! users were revealed. To compensate, Verizon cut $350 million from the original deal price.

To help the board avoid a similar situation, always assume there has been a breach. Then, conduct thorough research into the new entity, location, or partner and report on specific impacts, probabilities of occurrence and recommendations on how cyber risks can be addressed.

BUILDING A STRONG RELATIONSHIP WITH YOUR BOARD

Like any relationship, a successful partnership between a CISO and the board of directors calls for ongoing, proactive efforts on both sides. The goal is to establish and maintain mutual trust and confidence in the other party.

- Board members need to trust in your understanding of the organization and how cybersecurity affects business objectives, revenue generation and operations. Demonstrate this understanding by placing your presentations and other communications about cyber risk in a business context (finances, liability, compliance, reputation). Actively participate in all aspects of the business, from business development and vendor management to employee hiring and onboarding, so you are aware of potential risks and exposures.
- You need to trust the board to provide the budget and other resources you require to optimize the organization's security posture. Communication is fundamental, but so is familiarity. Help the board get to know your team, key technologies, and methods. Invite them to observe a security exercise or simulation. Such interactions will also help you determine the directors' level of security knowledge.

A strong relationship will pay dividends during a security incident, when you must depend on the board's backing of your requests for support and resources.

TRUST AND COMMUNICATION

Although this whitepaper focuses on leading practices for quarterly (and special) meetings with your board, our recommendation of putting cyber risk and security into a business context applies to any type of communication with directors. Ideally, you will find many other opportunities to interact with the board. Regular communication and an atmosphere of mutual trust will help you achieve greater protection and business resilience in the face of changing threats.

> **"...The CISO-board relationship is one of the most critical dynamics in business today. The organization's future depends on it."**
>
> - SecurityIntelligence.com[3]

ABOUT PONDURANCE

Pondurance delivers world-class Managed Detection and Response services to industries facing today's most pressing and dynamic cyber security challenges including ransomware, complex compliance requirements, and digital transformation accelerated by a distributed workforce. By combining our advanced platform with our experienced team of analysts we continuously hunt, investigate, validate and contain threats so your team can focus onwhat matters the most.

Pondurance experts include seasoned security operations analysts, digital forensics and incident response professionals, and compliance and security strategists who provide always-on services to customers seeking broader visibility, faster response and containment, and more unified risk management for their organizations. Visit Pondurance.com for more information.

Sources:
1. Cybersecurity Reporting: Future Considerations For Board Members, Corporate Board Member, 2021.
2. Corporate boards: Don't underestimate your role in data security oversight, Federal Trade Commission, April 2021.
3. Five Ways to Improve the CISO-Board Relationship, Security Intelligence, March 2017.