Microsoft Security

The CISO's Guide to Successfully Meeting with the Board of Directors

Tips on Researching, Strategizing, and Presenting Your Company's Information Security Status at the Highest Level

Table of contents

Introduction

1. How boards view cybersecurity
2. Presenting to the board
3. Illustrating risk
4. Ways to assess your meeting
5. High-impact examples

Conclusion

Introduction

Why boards are increasing their attention on information security

As a CISO, you have complex responsibilities. You work in a highly technical field where the parameters are constantly changing. Even for a security professional, it can be a challenge to keep up to date. And yet there are times when you're called upon to explain what you do and why it matters to people who may not have a technical background—people who are seeking to understand not only the value of your work, but how it fits into the functioning of your company.

You know that the financial risk is too large to ignore. It's been projected that within the next four years the cost of cyberattacks will reach a staggering $4.61 trillion.[1]

So how do you communicate to business decision-makers the critical importance of information security? This guide is here to help.

The media coverage that now follows high-profile attacks has underlined the need for robust security to business leaders at all levels. But another compelling factor may be the new laws which are assigning personal liability to the members of corporate boards. If board members are personally found to be negligent in the area of information security, they can face a significant financial penalty.

When the board is looking for insight on cybersecurity issues within their company, the CISO is the person best positioned to convey that information—which is why it's becoming more common for CISOs to be invited to make presentations at board meetings.

Some board members may be aware of a CISO's title and responsibilities. However, providing a clear understanding of how the information security department functions can help them decide how to integrate security into the company's strategic initiatives.

A new opportunity

For many CISOs, being scheduled to meet with their board can raise a host of issues. The board is not a group he or she normally reports to. It's easy to wonder if the board thinks something needs to be fixed. Or maybe they're going to ask questions the CISO might not have immediate answers for.

Meeting directly with the board can bring many positives. Once a CISO is familiar with a board's expectations, an initial presentation can be the start of a beneficial relationship for everyone involved. We've created this resource to help you do just that.

As a CISO, you can use this guide to help determine your board's expectations, use the language they understand, and open a line of communication that will win their confidence. Along the way, you will build the support of your executive team and bolster the visibility of your department.

① How boards view cybersecurity

As catastrophic ransomware attacks and large-scale data breaches that make headlines have raised awareness, boards are turning more attention to data security.

But it's more important than ever for board members to understand how these incidents relate to their role in managing overall risk.

Oversight that's high level and long term

At a basic level, a board will most likely include inside directors—like the CEO and other C-level executives—and independent directors, outside members who are likely executives in other companies and can serve without conflict of interest.

In general, the board is tasked with setting high-level strategy, overseeing executive management, and protecting the interests of the shareholders.

View of risk

It's been said that a board views everything through the lens of risk. There's no way to eliminate risk entirely, nor would that be desirable. In business, there's no reward without risk. However, risk can be managed.

A board can best understand the role of cybersecurity when it's presented to them in terms of specific operational risk, and when it's explained in terms of how it directly affects profit-making activities. When presenting to the board, focusing your presentation through this lens can be helpful.

Gathering background

The number one rule of public speaking is "know your audience." In preparing for an initial presentation to a board of directors, a CISO can gain an advantage by getting familiar with each of the members, which can allow them to address the members by name and tailor the presentation for the best reception.

Most company websites list the board members along with basic information about their business backgrounds and where else they serve in leadership. It's possible to dig a little deeper into the publicly available information easily accessible on each and may enable the CISO to give examples that individual members may be familiar with.

Finding an ally

Learning about the individuals who comprise the board will help a CISO gain another key component in a successful relationship—establishing contacts. A CISO is already working with their CEO and other board members from inside the company, but it can be helpful for CISOs to communicate with C-level executives outside of official meetings, especially as they can help to make the most of the all-too-brief time available in the meeting.

Building relationships with independent board members can bring benefits as well. Requesting a brief opportunity to speak with them individually in advance of meetings—to answer questions or explain context—can help create a situation where everyone comes to the meeting with a clearer understanding and can be more productive as a group. Since board decisions are built on consensus and trust, this can enable that process by putting everyone on the same footing. And when a board member has interacted with a CISO on security topics outside the meeting, he or she can become a conduit for ongoing discussions around security.

For this reason, a CISO may choose a board member who has some experience in cybersecurity, then reach out to them for an informal meeting.

② Presenting to the board

When presenting to your board, it's helpful to alert them to red flags concerning security and the ways they can be forward-thinking in mitigating potential business risks.

Your board's meeting time is most likely constrained. To get through what may be a sizable agenda, members find it useful to quickly distill discussions to the essentials.

In terms of cybersecurity, a CISO can help the board focus on those essentials, including how to manage risk, how an incident may affect key business activity, and how effective data security can foster new opportunities.

7 tips to ensure an effective presentation to the board

These suggestions for creating effective communications to your board are based on our own experiences presenting to the various boards and committees that govern Microsoft enterprises.

1 Research

Find out in advance from allies on the board what the board wants and needs to hear. Learn which areas of risk they're most concerned about. Check with your CEO and other inside members, then prepare the information that will help them make their best-informed decisions.

2 Overprepare

Because board time is valuable, coming in fully prepared can ensure you have a chance to make all your points. Hone your presentation to its most essential form. Create your slides and write your script, then ask a board ally to watch you run through it. Have them list the kinds of questions that are likely to arise.

Preparing additional information beyond what you anticipate presenting can be productive if the discussion gets extended by interest from board members.

3 Include the executive team

You can avoid surprising your CEO and other company executives on the board by sharing your presentation with them ahead of time.

It's also a good idea to keep other key executives involved in data security apprised of the issues you'll be discussing. Making sure they know that information security challenges your company is facing are being properly surfaced through the chain of command builds their confidence in you and in the company.

4 Tailor the message

Given their busy agenda and the reams of data presented to them, board members are most likely to retain the information they find useful in fulfilling their role. So be sure that you frame your presentation points in terms of high-level goals and risks.

When talking about your department's current or planned efforts, make a business case for your initiatives.

5 Use examples for impact

In the CISO's world, discovering that a hacker has created a successful backdoor exploit using a maintenance hook is the stuff of nightmares. But it may not strike a chord with board members—until they understand its impact on profit and loss. When you include example data breaches in your presentation that reflect the business consequences of the attack, it can help your company leadership better understand the overall risk.

The best examples will involve incidents that happened to companies similar to yours, or a company that a board member has a relationship with. They can vouch for the reality of the risk.

6 Frame SecOps as a tool for growth

Board members may not be aware of the possible connection between managing information risk and being better prepared to boldly seek new opportunities.

An illustration of this counterintuitive principle is how the increased braking power of a Formula One® racing car allows it to go faster around the track. Because the driver is confident he can quickly control his speed heading into the turns, he can go faster on the straightaways and so drive at a higher average speed.

7 Maintain focus

Hopefully, your meeting with the board feels informal and relaxed. But avoiding casual asides and sticking to the presentation you've planned will help ensure all your points will be aired.

And there's an even more important reason not to extemporize: Anything said in a board meeting is entered into the official minutes. Your offhanded remark could inadvertently raise an issue that could be better dealt with directly through your executive team.

A good rule of thumb is to avoid surprises. If a CISO is aware of a significant issue, they should try to resolve or at least address it before they are potentially asked to report on it to the board.

③ Illustrating risk

Discussions around data security can seem abstract and confusing to those not familiar with the technical ins and outs. Using real-life examples of data breaches and their consequences can help a board see the importance of taking risk seriously.

As mentioned in the last section, it can be beneficial to choose example incidents that are relatable in some way—for example, those that occurred at a company similar to yours. This will help a nontechnical audience more easily understand and appreciate what happened.

Walking through a high-impact example

When example incidents are presented as compelling narratives, it can make them more memorable.

1 Choosing a relatable example

The ideal case study of a data breach will be one that hits close to home. Look for companies similar in size and operations to yours in order to help board members realize, "Wow, that could have been us."

2 Walk through an example incident

When presenting an incident that's relevant to your company, it's good to state explicitly why it was chosen.

As you give the details of the vulnerability that allowed the breach, the method used to exploit the opportunity, the company's response, and the consequences, make it an interesting story. Who were the people involved? What did they do? What were the long-term consequences and impacts?

3 Conclude with what's been learned

If your story has its intended impact, the next thing the board will want to know is how your department is managing the risk of similar attacks. Have a thorough answer ready. Most of all, be sure your team really is prepared for a similar incident.

This is an area well worth discussing before the meeting with allies on the board.

④ Ways to assess your meeting

When a CISO is well prepared for their first board meeting, the board will likely notice.

However, there are always areas for improvement. By doing an after-meeting assessment, a CISO can ensure that the next meeting will go even more smoothly.

Going from good to great

1 Finding out how it went

Sometimes it's hard to tell during a presentation whether it's being well received. After the meeting, you can touch base with any executive team members who were present to get their impressions, and then ask your allies how they thought it went. Ask for specific examples of what seemed to resonate with other board members, and what could have gone better.

You might ask what would be an appropriate follow-up to the information you presented. For example, you might create a one-sheet executive summary of the major points surrounding your company's data security that they should be aware of.

2 Preparing for your next presentation

With cybersecurity now recognized as a significant area for risk management, it makes sense that your board will want to hear from you on a regular basis. Prepare for your next meeting by staying in touch with your board ally, and be on the lookout for good incident examples and relevant research.

3 Making it a process

Hopefully, your initial interaction will have made the board realize that information security risk is not something that can be fixed once and for all. It's a constantly evolving process. So let them know that you're available to give high-level status reports on a regular basis. Offer to get on their calendar as frequently as they require.

Additionally, you can offer to be a resource outside the meetings. For example, you can make yourself available to be part of the onboarding process for new board members.

⑤ High-impact examples

As mentioned earlier, there's a chance that some board members will have direct experience in cybersecurity. But it's likely that most of them won't have the technical understanding or familiarity with the safeguards and procedures you use to protect the company.

Taking the board through some brief activities can help them accurately see the complex nature of the threats and better perceive how the information security team is taking them seriously.

These activities can be completed in a few minutes and help sharpen your presentation to your board. In each case, it would be good to create a one-sheet infographic summary to leave behind.

1 Let's walk step-by-step through a hypothetical incident at our company.

Take them from detection through resolution, describing the key people and processes involved.

2 How we assess our threat exposure through our vendors.

Your board may not be aware of the risk that improperly protected vendors can pose. Briefly describe the kinds of risks you look for and how you manage them.

3 How we prepare against AI-based threats.

AI threats are in the headlines, so your board is probably generally aware of them. But they most likely don't know the specifics on how bad actors are using them. You can start with an example of how bad actors are leveraging AI for convincing social engineering traps, and end with how your team reacts when employees inadvertently fall prey to one of these traps.

4 How we handle a privacy breach.

Your board knows that all risk is not created equal. For example, there's a big difference between an attack that threatens operations versus one that merely damages the company's reputation (e.g., release of customer personal info).

Walk them through your team's technical response and then take them through how you work with public relations to announce the breach.

Conclusion

Going from initial presentation to productive relationship

With boards taking a greater interest in information security, CISOs like you are being asked to appear at board meetings. This is an excellent opportunity for you not only to bring the board up to speed but to establish a good working relationship.

The advice in this guide is designed to help you prepare for an initial meeting. By doing thorough preparation, you'll be able to interact more effectively with this audience, and you'll be much more confident at the meeting.

When a CISO can help the board see how their department is contributing in terms of big-picture risk and reward, they can become a trusted resource as they provide high-level guidance for their company.

Find more information on how CISOs can effectively work with company leadership

[1] "Microsoft Copilot for Security generally available on April 1, with new capabilities," CEE Multi-Country News Center, March 15, 2024