AVERTIUM

WHITEPAPER

Strengthening Cybersecurity with Consensus:

How to Build Positive Board Relationships

AVERTIUM. SHOW NO WEAKNESS™

Table of Contents

Introduction

In 2019, the World Economic Forum ranked cybersecurity as one of the top five greatest threats to world economies and stability. Executives are taking note, given that a major breach carries an enormous price tag in terms of fees, intellectual property (IP) losses – and irreparable brand damage. And *with CEO departures following most major data breaches*, they're far more aware of their own liability in the event of any kind of security incident.

With cybersecurity ranking as one of the top five greatest threats to world economies and stability, the CISO must now take a seat at the board table and learn to communicate best practices while justifying new protocols and expenditures in business terms.

But as cybersecurity becomes a greater priority in theory, actual practices have some catching up to do. Many enterprises still lack basic security practices like implementing multi-factor authentication (MFA). Furthermore, the threat of attack is constant, and a breach could happen at any time. That means that monitoring, prevention and response protocols must be constant as well. Increasingly, executive boards are turning to the chief information security officer (CISO) for guidance and execution of a thorough security program that delivers demonstrable business value.

Already tasked with the ongoing protection of critical systems and sensitive data, the CISO must now take a seat at the board table and learn to communicate best practices while justifying new protocols and expenditures in business terms. This is on top of existing security training the CISO oversees, as well as needed system patches, coordination of security teams and access management across the enterprise, to name just a few core responsibilities.

While there are many priorities vying for the CISO's attention, successful communications with the board are now the most critical to job security. In other words, it might be a new task on the list, but maintaining positive board relations is at the absolute top.

The CISO must be able to effectively convey the following:

- The extent of an organization's risk
- Present and future strategies to mitigate that risk
- Easy-to-digest metrics that prove the business value of current security spend
- A compelling case for the necessary financial support moving forward

If you're a CISO tasked with joining or presenting before your company's executive board or board of directors, we're here to help you develop a comprehensive and effective approach to building board consensus. That way, you can successfully execute the highest level of security protocol at your organization.

Cover Your Bases for Effective Board Presentations

There are two basic initial steps to success: Know your audience and know your approach.

> 59% of organizations say the relationship between cybersecurity and the lines of business is at best neutral, to mistrustful or non-existent.
>
> - Global Information Security Survey 2020 Report

First, let's talk about the audience - your board. An executive board is a group with C-level titles, such as CEO, chief information officer (CIO) or chief operating officer (COO). This type of board is both overseeing daily operations and creating overarching strategy and policy. A board of directors, by contrast, can include both executives and industry experts from outside the company. This body represents the company's shareholders, so they're interested in maximum returns and minimal costs.

Overall, both types of boards want the answers to the same basic questions: *What's our level of risk, what's our plan – and how much will it cost?*

The board can seem intimidating, but they're really just a group of people with their own professional responsibilities and areas of expertise.

- ✓ Do your research to understand their perspectives and build rapport well before your security presentation.
- ✓ Make the effort to reach out and initiate individual conversations on the topic of security.

You can gauge your fellow executives' level of understanding and address some concerns one-on-one. This builds a sense of trust and confidence so that when you're making recommendations, the board already has a wider context to understand your thinking – and your requests.

Similarly, it helps to provide these groups with a preview of any presentation content so they know what to expect. Creating a short list of key topics of discussion also forces you to organize your ideas and come prepared to succinctly present your points and then address any lingering questions. If you can't adequately alleviate the board's concerns, support will constantly be an uphill battle and you will not be able to build and/or accelerate a successful security program.

How to Present to the Board

Now to the presentation itself. A simple barometer is the following: *Would I want to listen to this presentation after – or during – a long day? Would my neighbor?*

The technology field is rife with acronyms to shorten complex and lengthy terminology. But those unfamiliar with their meaning can quickly get lost in the alphabet soup and tune out.

- ✓ Aim to simplify your ideas by eliminating jargon and defining your terms with easy-to-grasp examples or analogies. Board members will not approve what they can't follow.

- ✓ Extend the same standards to your visual aids. Make sure you organize your data visually to tell a story that can be grasped in a glance.

Note: Be careful not to overdo the doom and gloom. Frightening statistics and cautionary tales will not help you to achieve your – or their – key objectives. Executives are aware of the greater stakes at play; what they need is a clear understanding of which strategies will best mitigate risks and ensure compliance.

Executives are aware of the greater stakes at play; what they need is a clear understanding of which strategies will best mitigate risks and ensure compliance.

- ✓ Be prepared to keep the focus on action items tied to measurable business outcomes.
- ✓ Back up any claims with visualized data and reputable third-party sources.

What to Present

Organizing your thoughts and using this time wisely is crucial in getting your message heard and considered. At a minimum, you must cover the following:

- Policies and procedures to meet compliance with required frameworks (NIST, ISO, COBIT), legislative standards (Sarbanes-Oxley, HIPAA, Gramm-Leach-Riley) and industry-specific requirements (PCI, EMV)
- Use of advanced security technologies (application aware firewalls, SSO, network DLP, advanced malware response, public cloud security, managed security, etc.)
- Data loss prevention tactics
- Data encryption for all types (mobile, desktop, email, hard drives, etc.)
- End-to-end security protocols across cloud, mobile, remote environments and other layers
- Detection methods

This information will help you and the board form an overall risk appetite, or level of risk tolerance, and corresponding assessment. They will want to know how these measures compare to industry peers, whether they're in line with the latest security trends and what gaps in protection exist (along with the potential ramifications of those gaps).

Leave No Vector Undetected

As companies grow and develop new business relationships, they increase the number of entry points across their network. Those entry points then become new attack vectors. . Social media accounts, for example, are not top-of-mind in terms of cybersecurity, but are subject to danger.

These outlets must be monitored for any suspicious activity, especially the creation of fake (yet convincing) accounts by bad actors.

- ✓ Be sure to convey the full extent of your organization's vulnerability.
- ✓ Be certain your security plan is scalable and includes plans for future measures.

Address Third-Party Risk

Another attack vector that must be addressed is that created through third-party vendors. These outside companies with access to your internal network open your company to new threats, particularly when their infrastructure is less secure than your own. In 2013, hackers stole more than 40 million credit card numbers from Target by exploiting the weakness of their HVAC company's security.

One solution for reducing this type of vulnerability is supplying vendors who need access to your network with company computers that have proper security tools. Some companies find it useful to create a designated cybersecurity committee to regularly review, adjust and implement this type of policy.

BYOD

Regulating network access inside your company is another important point of consideration when assessing risk. The bring-your-own-device (BYOD) trend, once popular for its convenience for employees and IT budgets, creates even more attack vectors across your network. Equipping employees with company devices that you can lock or wipe remotely brings an added layer of data protection should those devices become compromised or lost. You will need to help the board understand the potential risk tradeoff involved in allowing employees to access needed data from their personal devices.

A word of caution: A BYOD policy is complex and the line between privacy and security becomes blurry. Thoroughly investigate this option to determine if it's feasible and fits your risk appetite before proposing this approach to the board.

Insider Threats

Indeed, a company's own employees often present the greatest threat to cybersecurity. Verizon's 2019 Data Breach Investigations Report found that of the incidents studied, 80% were the result of phishing – and 94% of malware arrived via email. Too many phishing attempts succeed due to carelessness or a lack of proper understanding on the part of employees.

Regular educational training and communications programs across the enterprise are a simple, yet effective, way to mitigate employee risk. Employees must also feel safe in reporting accidental missteps and not fear being disciplined or fired. Begin by building a safe and informed culture from the board level down with executive understanding and support.

Establish a Mutual Mindset of Resiliency

Building consensus with the board is a two-way street. For your part, you need to take the time to understand your organization's business model and translate security efforts as they relate to the bottom line. Does the security program you're overseeing empower greater business goals? Does the program increase revenue and reduce costs?

You will also have to work closely with board members to help them to establish the right expectations based on the latest technologies and thinking around cybersecurity approaches. It's critical to establish the proper security mindset amongst all teams. Board members need to understand that some level of breach is inevitable. In the words of Joseph Demarest, assistant director of the FBI's cyber division: "You're going to be hacked. Have a plan."

The focus of a cybersecurity program must be one of resilience rather than all-or-nothing prevention. A recent report from the Directors and Chief Risk Officers Group (DCRO) recommends that organizations leave behind a "prevention-only" approach and instead operate from the assumption that a breach has already occurred. For boards, a key first step is identifying which valued company assets are core and need the highest level of protection.

From there, what does a security program based on resiliency look like? The DCRO recommends a three-pronged approach:

1. Threat intelligence and threat modeling
2. Testing defenses and reactions
3. Practicing what-if scenarios should these reactions prove unsuccessful

Use these questions to break down how you might communicate this information with shareholders:

- What is the response plan for breaches and other security incidents?
- Have you tested said plan?
- What is your testing method?
- How will incidents be communicated across the organization (Think: employees, shareholders, media, lawyers, customers, law enforcement and partners)?

In keeping with a resiliency mindset, cyber insurance policies are another important safeguard against major financial losses. Coverage can include:

- Third-party exposures
- Breach expenses
- Extortion threats
- Media liability
- Business interruption

Your company's corporate insurance policy may not include cybersecurity, so corporate insurance departments will need to review the extent of coverage to determine the need for an additional rider or a separate policy.

And don't forget to prepare your own response post-breach or incident. Are you ready to discuss a security incident in front of the board? You'll need to address the issue proactively and head-on, since it will be top of mind for everyone. From there, many of the same presentation guidelines apply:

- ✓ Focus on facts and be transparent.
- ✓ Explain your response in a step-by-step manner.
- ✓ Be prepared to articulate the incident's economic impact with up-to-date, accurate figures.

A Culture of Cybersecurity

An aligned organization has the potential to be a prepared and resilient one. In addition to specific strategies and tactics, a culture that values protecting the company is a cybersecurity program's greatest asset. The more you can educate your board and build consensus, the easier it will be to grow your security program. Furthermore, employees who feel engaged and appreciated at their jobs are less likely to compromise company assets.

Also, if you regularly engage the CIO or CRO at your company, you can better avoid competing budgets and adversarial tensions. Shared initiatives with other C-level executives make for smoother implementations of meaningful protocols.

In Conclusion

New and persistent threats call for coordinated security programs equally focused on prevention, detection, and recovery. By learning to speak the language of your executive board, you can help educate them on pressing security issues while advancing a comprehensive cybersecurity strategy that delivers measurable results for your organization.

About Avertium

Avertium, one of the largest cybersecurity services providers to the mid-to-enterprise market, is redefining the landscape with its distinctive show-no-weakness approach. Forged out of three award-winning cybersecurity services companies, each with a unique perspective on the security landscape, Avertium brings enterprise-level security to the many mid-sized and larger organizations that don't have access to comprehensive, specialized protection. More than 1,200 organizations in industries ranging from financial services and manufacturing, to technology and healthcare benefit from Avertium's managed security, consulting and compliance services delivered with more rigor, more relevance, and more responsiveness. The company's dual security operations centers are located in Arizona and Tennessee.

Avertium. Show No Weakness.™

AVERTIUM

StrengthenCybersecConsensusWP_0720

+1 (877)-707-7997
hello@avertium.com
www.avertium.com