EBOOK

How to Communicate the Value of Cybersecurity to the Board of Directors

A Guide from the Managed Services Experts at TPx

TPX

EXECUTIVE SUMMARY

The cybercrime industry is booming, with cyberattacks becoming more sophisticated, frequent and profitable. In response, businesses must invest in cybersecurity and protect vital data and systems from bad actors. IT knows this all too well, but does the board of directors?

Securing board buy-in on cybersecurity investments is crucial, but the path to success isn't straightforward. This eBook highlights the disconnect between IT and the board and provides guidance for gaining alignment.

Key Takeaways

The board of directors must understand the value of cybersecurity so it can make informed decisions and protect the business.

Cybercrime is successful and attacks are becoming more complex and harder to combat.

Every employee has a responsibility to maintain good cyber hygiene.

Convincing the board of directors requires strategy and well-reasoned dialogue.

Working with a managed services provider can offer effective cybersecurity and reduce investment in money, talent and time.

Table of Contents

Part 1: Why Do Boards Need to Understand the Value of Cybersecurity Investments?

As part of the IT team, you already understand the need for cybersecurity investments to keep pace with cyberthreats and cybercrimes as they shape-shift and evolve.

Communicating the value of continuing cybersecurity investments to purse holders has always been a challenge, but it can be particularly so when discussing with the board of directors. Why?

- Everyone comes to the table with their own interpretation and perspective on cybersecurity and cybersecurity awareness.
- Boards may have technologically fluent members, but most aren't flush with technology and cybersecurity experts.
- Technical jargon can get in the way of meaningful dialogue.

Today, boards must understand the value of cybersecurity investments because more is at stake than ever. Board members may not have daily business

responsibilities, but they do have fiduciary oversight. Board members can also be held personally liable for inaction that leads to a cybersecurity breach.

Additionally, impending changes in compliance and oversight at the Securities Exchange Commission will soon require companies to disclose their cybersecurity governance capabilities, including the board's oversight. Specifically, companies must disclose:

- Whether the entire board, specific members or a committee is responsible
- The processes used to inform the board and the frequency of discussion
- Whether and how the board, or specified members and committees, consider cybersecurity part of its business strategy, risk management and financial oversight

How do you get the board on board with cybersecurity?

Communicate the need to invest in cybersecurity in ways that resonate and align with the board. Focus on risk, resiliency and reputation, not technical firepower. If you can mitigate risk, develop resiliency in the face of a breach and manage your reputation, the return on investment (or value) is clear.

What is the board's role in an organization?

Governance
The board is the governing body of a company and is typically elected by shareholders. Public companies must have a board in place, though private companies and nonprofits may also have boards.

Fiduciary
The board meets regularly to make fiduciary decisions for the company on behalf of shareholders to entertain mergers or acquisitions, offer dividends, set pay and hire or fire senior-level staff.

Goal-Oriented
The board also sets company goals, supports senior-level staff in reaching them, and ensures the company has the financial resources to achieve them.

Independence
Boards usually comprise the company CEO, senior managers and outside members not affiliated with the firm. NYSE and Nasdaq require listed companies to have a board with a majority of directors independent of the company.

What does the board need to know about cybersecurity?

Risk Management vs. Financial Viability
The board is simultaneously responsible for managing risk to the organization and ensuring profitability and financial viability for the company.

Technical Knowledge
The board doesn't need complete technical expertise but must know enough to make decisions effectively and manage risk appropriately.

Clarity & Insights from IT
Boards don't understand effective cybersecurity risk management and perceive it as an overly complex issue requiring clarity from IT leaders.

What are common misconceptions the board may have about cybersecurity?

MYTH 1 Only Tech Businesses Need Security
Cybersecurity isn't only for certain businesses, like those in tech or with PII or regulatory requirements. All companies need cybersecurity.

MYTH 2 Antivirus and Firewall Are Enough
To combat today's cyberthreats, companies need a comprehensive solution with more security components than simple antivirus and firewall.

MYTH 3 Supply Chain Attacks Aren't a Threat
Cybercriminals target supply chains to get inside a business network. Take action to ensure secure communications and collaboration.

MYTH 4 Cybersecurity Threats Aren't Preventable
While no company can guarantee 100 percent protection from cyberattacks, you can still safeguard your operation and mitigate substantial risk.

MYTH 5 Employees Can't Mitigate Human Error
Human error will always be a concern, but effective security awareness training can empower staff to help avoid data breaches.

Part 2: What Are the Current Cybersecurity Challenges the Board Needs to Know?

Board directors must be aware of several challenges with cybersecurity so they can respond appropriately and intelligently.

Cybersecurity Is a Living Practice
The threatscape is evolving, with vulnerabilities, ways to attack and defense strategies constantly responding and adapting.

Cybercrime Is Organized & Highly Profitable
Cyberattacks are increasing in number and sophistication. Here are three big reasons why:

1. Cybercrime is becoming productized. It's also an industry. So, one group can identify vulnerabilities and collaborate with another group of threat actors to penetrate an organization.
2. These groups, in turn, can sell the ransomware "as a service" in exchange for a cut of the profits, extending the accessibility of cybercrime extensively. With profitability so high, organized crime has also entered the scene, making attacks more powerful and frequent.
3. It's not just hackers in the basement. Nation states are capitalizing on this new revenue stream by protecting or supporting cybercriminals.

Every Industry & Vertical Needs Cybersecurity
In the recent past, only highly regulated industries, like finance and healthcare, prioritized cybersecurity. Now, organizations of any scale and in every sector are vulnerable to attack, including manufacturing, retail, energy infrastructure and education.

The Way & Where We Work Have Changed
Remote and hybrid work strategies have become commonplace, dramatically increasing cybersecurity vulnerabilities with networks and workers spanning multiple platforms and locations. The more digitized work processes become, the more avenues for cyberattacks become available.

As work situations change and cybercrime becomes an industry, leadership (including the board of directors) must be aware of the dangers and understand the importance of continual investment in cybersecurity.

Part 3: Who Is Responsible For Cybersecurity?

Everyone is responsible for maintaining good cybersecurity practices — from your tech team to your C-suite to new employees.

How Are the Different Members of Your Organization Responsible?

General Staff

Cybersecurity is an issue for an entire organization and needs a holistic approach.

Aligning all employees, not just the cybersecurity team, around practices and processes to keep the organization safe is not a technical problem — it's an organizational one.

Many cybersecurity problems occur because of human error. Cybersecurity requires awareness and action from all members of the organization to recognize anomalies, alert leaders and ultimately mitigate risks.

Creating a culture that promotes cybersecurity and awareness and empowers individuals to behave like security chiefs adds a layer of protection to avoid, detect and report any behavior that can lead to a threat situation.

Tech Leadership

The CTO, CIO and IT team have a key role in educating and enforcing healthy cybersecurity habits. However, they shouldn't be expected to handle cybersecurity siloed from the rest of the organization. Their leaders and teammates need to support them and listen to their guidance.

Board of Directors

The board of directors, like the general staff, must exhibit high levels of cybersecurity awareness. In fact, many cyberattacks are targeted against business leaders for access to critical data, so leaders should be extra cautious. Additionally, the board of directors must oversee the implementation of cybersecurity policies and listen to the cybersecurity team's guidance.

Part 4: How Do You Position Cybersecurity to Your Board?

Your board of directors must know specific information about cybersecurity and your cybersecurity initiatives. You will need to be able to answer the following questions:

What are the company's most important assets, and how are they protected?
Important assets most often include:

- Intellectual property, such as proprietary software and patents
- IT infrastructure, including servers, networks and data centers
- Customer data
- Brand reputation

Assets are best safeguarded through a multilayered security strategy:

- Physical technology and hardware are protected by restricting access to critical infrastructure, such as data centers.
- Digital operations are secured by implementing security solutions like firewalls, encryption and intrusion prevention systems (IPS).
- Business leaders instill good cybersecurity practices through staff training, well-defined cybersecurity policies, regular audits and third-party vulnerability assessments.

How are breaches detected?

- Most security breaches are identified by external sources rather than affected businesses.
- Businesses can identify internal breaches through Intrusion Detection Systems (IDS) to monitor network traffic for suspicious activity.
- Evidence of a data breach can include sudden changes to admin account information, strange files in your system with unknown sources, leakage of customer or company information, unusually slow networks and suspicious network activity.

What are response plans?

Cybersecurity strategies include response plans to allow for quick, effective remediation of breaches or vulnerabilities. Plans generally follow these steps: isolation, investigation, notification, rectification and review.

What are business recovery plans?

Business recovery plans are implemented to quickly restore essential functions after disruption. Recovery usually includes data backup and restoration, alternative operational strategies and defined communications protocols.

What role does the board play?

The board generally provides strategic oversight and ensures cybersecurity plans align with business objectives. Additionally, they're responsible for allocating appropriate resources to cybersecurity initiatives and assessing overall effectiveness.

Is your investment enough?

You can't invest enough to become 100% secure against cyberattacks. But, budgets must be set and approved. It's important that the board evaluates the level of protection against their risk tolerance and comes up with a budget with which they're comfortable.

Part 5: What Are the Steps to Get Board Buy-In on Cybersecurity Investments?

There is no golden ticket to ensuring board buy-in, but here are some steps you can follow to help you along:

1 Build a strong business case.

You need to identify the cybersecurity risks your business faces, the potential impact of cyberattacks on your business, the data breach cost, and how cybersecurity supports the company's goals and objectives.

2 Create a dialogue to engage leadership and build trust.

Leadership values accountability. They want more than a briefing — they want to have a dialogue. Even though they're not involved in daily operations, the board still has overall responsibility and potential liability. Establishing a back-and-forth exchange sets a healthy foundation for further discussion.

Give your board a clear view of threats and vulnerabilities, how they could impact business, and a rundown of established strategies and investments and their predicted ROI.

Explain that cybersecurity is more than protecting data. Data is still a concern, but with more systems and processes online and controlled remotely, there's more at stake.

3 Choose the right narrative.

Boards may meet as seldom as once per quarter, so clearly illustrating your point is important.

- One way is to identify a recent threat, outline the measures taken to detect it and prevent a breach and then describe the impact it might have had on the business.
- Another tactic is discussing uptime, recovery and their costs in real dollars as opposed to the "wolf-at-the-door" narrative.
- Additionally, it's always important to illustrate how your business compares to others in the industry.
- Mention cybersecurity and compliance regulations and standards for your industry and the penalties for non-compliance.
- Shareholders also now have expectations around cybersecurity governance and due diligence. Shareholders are less likely to invest in an organization they're unsure of the security posture.

4 Keep the dialogue simple and engaging.

While today's boards are more cyberliterate, they traditionally don't have technical backgrounds. So, choosing the right language and keeping explanations concise is critical. Less is more in these discussions. Boards need to see cybersecurity as not just an IT issue but as a critical business concern that affects the entire organization's well-being.

- Also, avoid technical jargon and acronyms; if you have to use them, be sure to explain them.
- Focus more on the "why" than the "what." Board members want to know the benefits and aren't interested in how the solution technically works.
- Back up your case with data, metrics and real-life examples.
- Identify your audience and tailor your message to your specific board's needs.
- Always be prepared for questions and objections.
- Ensure adequate follow-up by identifying action items, next steps and establishing the ongoing plan for communicating and tracking progress.

5 Use simple and clear presentations to visually support the argument for investment.

The reality is that in your meeting with the board of directors, you'll need to offer a true presentation, either in a Microsoft PowerPoint or Adobe Acrobat PDF format, that has direct visuals to support your points. While your board of directors will likely have a higher attention span and greater understanding of cybersecurity than the average business professional, they'll have distractions come up during your meeting – visuals can help them stay focused and reorient themselves if they have to step away from the meeting.

6 Offer data in your presentation that supports the need for specific cybersecurity solutions for your industry.

Bring up industry-specific statistics around security vulnerabilities and cyberattack data. These stats are usually attention-grabbing and will be key in establishing the need for cybersecurity solutions with your board. Reputable sources like Gartner, Forrester, Frost & Sullivan, other analysts and security industry publications are reliable and respected places to source this data. Pointing out vertical-specific use cases will help build the case as well. For example, retailers may be more prone to attacks directed at consumer credit card information, which is reputationally destructive. Also, ensure that you present all forms of cost, including financial loss, reputational damage, proprietary information loss, and regulatory fines and penalties. The reality is that all sizes of businesses are being targeted, but if your company is large enough to have a board of directors, you're definitely a target.

7 Present realistic funding requests and prioritize solutions accordingly.

You aren't going to get every security solution necessary to mitigate cybersecurity attacks to the fullest extent, especially if this is your first year seriously considering cybersecurity investments with your board. You have a limited budget and a limited window of time for cybersecurity solutions to be deployed and rolled out. Some solutions may need to wait until the subsequent fiscal year. For example, you may be able to secure funding for a comprehensive network next-generation firewall (NGFW) in year one and set aside funds for managed detection and response (MDR) on the network in year two.

8 Speak using financial terminology.

The board of directors at most companies is primarily concerned with real-world business outcomes of financials and expected return on investment (ROI). If your IT director is presenting to the board, they need to verse themselves in financial terms to clarify what the board is investing in. Probabilities of breach and risk scores are all great, but in the abstract, they don't matter much to board members. Use concrete language around business outcomes and firm numbers on cost savings in the event of a breach to create a business case for them.

Developing and presenting a cost-benefit analysis is advisable to show possible losses without the appropriate investment in security solutions.

9 Illustrate the long-term vision of the organization's cybersecurity posture.

In your presentation, outline what the vision for cybersecurity looks like for the next three to five years so the board understands what future funding requests may look like and how your organization is phasing in higher levels of defense. Be sure they know that since the cybersecurity threat landscape is changing, the company's plans must adapt to compensate for new threats. This will set the stage for bringing up cybersecurity again in future board meetings if this initial meeting is one of the first times security has been on the agenda. You can also bring in experts (like managed service providers) on security to help explain what the phases for each year look like.

10 Reassure the board that they'll have oversight of the cybersecurity process.

Your board will be wary of approving funding for initiatives they're concerned they may not receive regular updates on. Reassure them that even though cybersecurity is complex, your team will update regularly on the status of the rollout of cybersecurity initiatives and are willing to get into the weeds of deployment details if need be. The board has a fiduciary responsibility to ensure the investment is used properly, so lean into that to help secure approvals.

11 Flip the conversation.

Present cybersecurity in clever ways that will resonate with board members. For instance, framing it as a "how" instead of an "if" can cement its necessity in your discussions. You should also contextualize your arguments from a business perspective and emphasize the people involved, not just the technology.

12 Communicate on a consistent cadence with the board.

Garnering support from your board on implementing more invasive solutions or developing entire programs, such as a security awareness training (SAT) program, may require a larger ongoing education over the course of the previous fiscal year before funding is greenlighted. Keeping the board in the loop on new developments via email and in regular monthly or quarterly meetings can help make funding requests a foregone conclusion and less of an unexpected surprise.

13 Follow up after the board meeting with clear calls to action.

After your board meetings, follow up via email with well-defined next steps, recommendations for board involvement or further investigations and highlight any urgent matters requiring immediate attention or decision.

Part 6: How Does Investing in Managed Security Add Value?

Managed services providers (MSPs) deliver the talent, bandwidth and expertise required to monitor and troubleshoot your solutions 24/7. Here are some of the benefits:

Instant access to expertise

With managed services providers, you get immediate access to teams of trained personnel that are experts in deploying, managing and troubleshooting the security solutions that protect your business from cybercrime.

Reduced overhead costs

Managed services providers save you time and money by providing valuable resources, including educational materials, training, software and skilled specialists that you would otherwise have to procure and handle internally.

Affordable, predictable and scalable plans

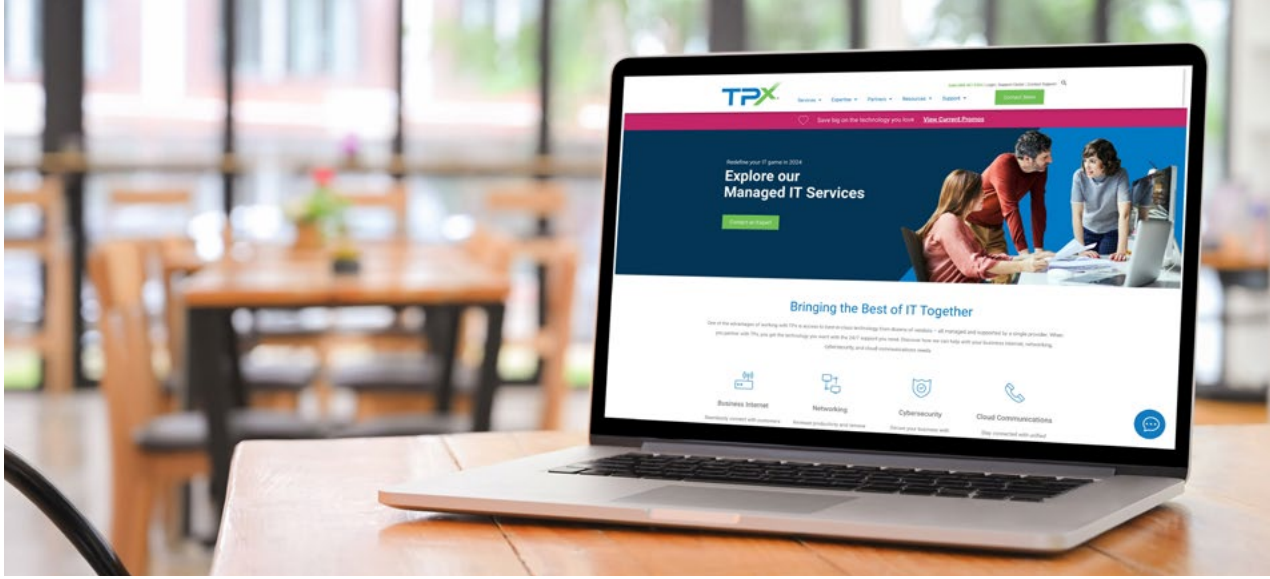
Working with a managed services provider can be less costly than developing and deploying cybersecurity resources internally. Moreover, MSP solutions are scalable and offer predictable pricing, giving you control over your IT spending.

More focus on your own business

Cybersecurity is a complex undertaking and an entire business unto itself. You can focus on managing and growing your core business by working with a managed services provider.

Part 7: Why Choose TPx?

You have enough business challenges. Partnering with TPx provides the support it needs so you can focus on core business goals. At TPx, we have the products, services, experience and certifications to keep your network and applications running smoothly and safely.



Why Choose TPx?

- Our mission is to be the easiest MSP to do business with.
- We solve the biggest IT issues – cybersecurity, connectivity and collaboration – under one umbrella.
- We have 120+ certifications across 60+ competencies, like CompTIA, Cisco, Fortinet, Microsoft, SMC and more.
- We offer HIPAA, PCI DSS and SOC 2-compliant solutions.
- We provide enterprise-class, 24/7 support.
- We offer different service levels and highly customizable solutions.
- We have a national footprint with multisite, multicarrier and partner coverage.
- With thousands of customers nationwide, we're big enough to get the job done and small enough to be agile.
- We have various dedicated teams to ensure service excellence.
- We continuously invest in automation, self-service innovation and back-office transformation.
- We are committed to providing the most densely monitored service-delivery platform in the industry.
- We understand and embrace the criticality of our customers' performance analytics.
- TPx is Your One-Stop Shop for Managed Services.

Essential “Must-Haves”

Backup and Disaster Recovery (BDR)
We help organizations quickly recover from system downtime and data loss caused by cyberattacks, human error, system failures and natural disasters. Using advanced hybrid local/cloud technology and skills management resources, TPx delivers a turnkey BDR solution that will meet your recovery objectives. All backups are scanned for ransomware and when a ransomware footprint is detected, you can roll back your systems as if it never happened.

Next-Generation Firewall (NGFW)
The firewall protects your network from internet-based threats. Next-generation firewalls block today’s advanced threats while providing secure access, visibility and control to help your business be more productive. TPx ensures UTM features such as web filtering, antivirus, application control, intrusion prevention and VPNs are properly configured, monitored and maintained.

Endpoint Management and Security
TPx helps keep your servers and workstations healthy, secure and performing optimally. Our endpoint security service leverages remote monitoring and management (RMM), patch management and security. Together with expert support personnel and security analysts, we provide an “always-on,” best-in-class, 24/7/365 service.

Managed Detection and Response (MDR)
Discover, prevent and recover from cyberthreats faster. TPx’s MDR helps you identify more threats, reduce attack dwell time, and proactively mitigate attacks. We offer managed detection and response for both firewalls and endpoints.

Strategic “Must-Haves”

Security Advisory Services
TPx advisory services provide comprehensive security consulting that can help improve your security posture and protect your business. Our services include a Virtual Compliance Officer (VCO) with a cybersecurity gap assessment, network vulnerability and penetration scanning, network security assessment, wireless security assessment and ransomware readiness assessment.

Penetration Scan
TPx experts show how exploiting a vulnerability could result in a significant impact on your environment.

Vulnerability Scan
TPx evaluates devices connected to the network to identify vulnerabilities present due to open ports, missing patches, etc.

Network Security Assessment
TPx evaluates your organization’s network security posture and profile.

Wireless Security Assessment
TPx evaluates your organization’s wireless infrastructure and configuration, security posture and functional capabilities.

User Security

Inbox Detection & Response (IDR)
TPx's Managed IDR service allows users to easily report suspicious emails with an Outlook plug-in to quickly determine if the emails are safe or malicious.

Security Awareness Training (SAT)
Users are your first line of defense. The more they know, the less prone they are to becoming victims of phishing scams or other security incidents. Our service includes monthly phishing simulations and Security Awareness Training courses with automated reporting to track your results.

DNS Protection
We protect systems and users from malicious websites using leading DNS protection software. Windows devices are protected both on the corporate network and while traveling. Network-based DNS protection covers BYOD, guest wireless, and non-Windows devices to deliver comprehensive DNS security and reduce your risk of attack.

Need Help With Cybersecurity?

CONTACT US

ABOUT TPX

TPx is a nationwide managed service provider helping organizations navigate the growing IT complexity. Founded in 1998, TPx offers comprehensive managed IT services including internet, networks, cybersecurity, and cloud communications. With a focus on service, TPx is dedicated to the success of its customers by making IT easy with solutions that address today's evolving technology challenges. For more information, visit www.tpx.com.

For more information

tpx.com