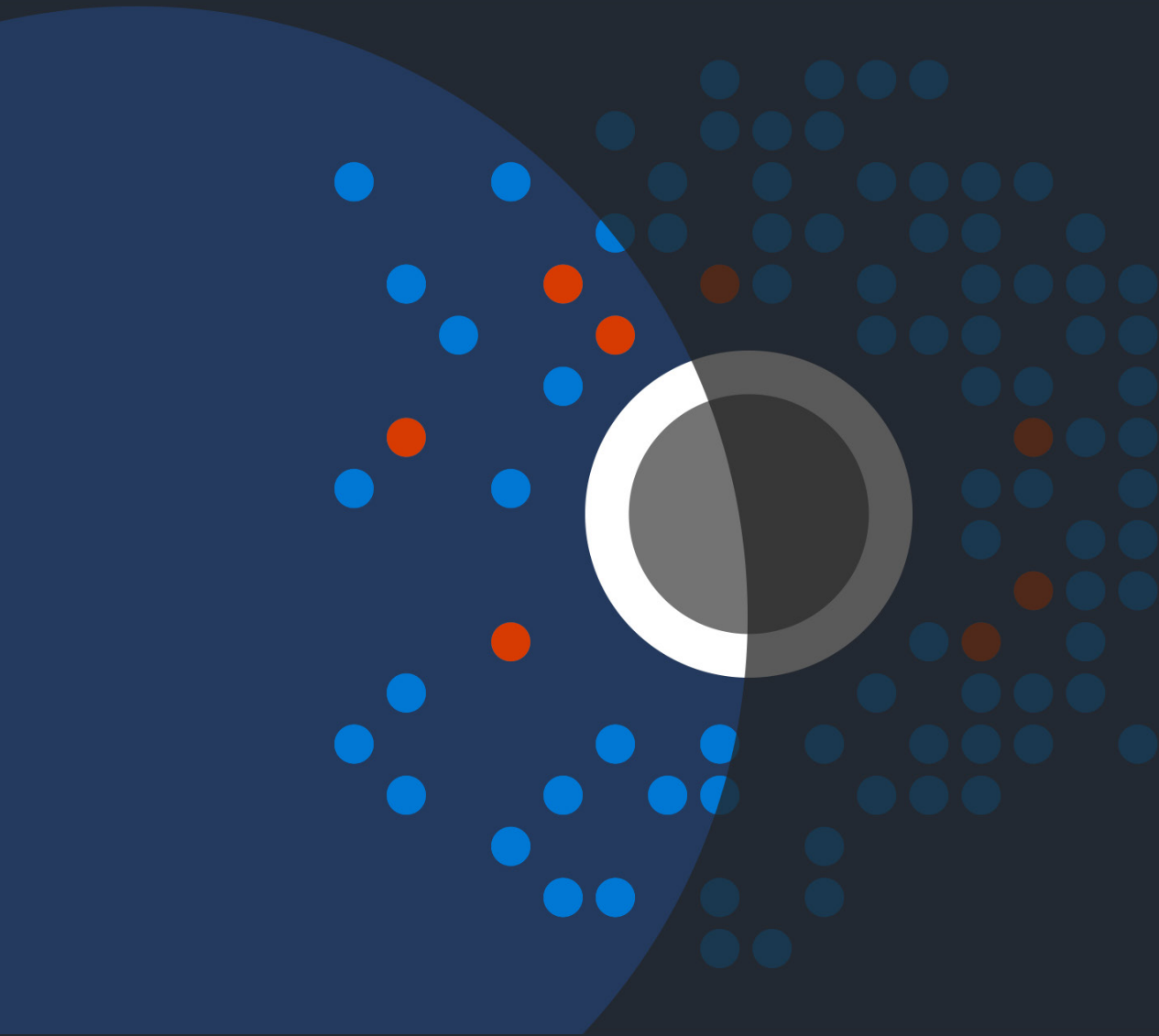Microsoft Security

The Cost of Inaction

A CISO's guide for getting boards of directors to invest in cybersecurity

As a CISO, nobody understands the security risks that your organization faces better than you. You've got the technical expertise to deeply appreciate current threats and how they stack up against your organization's vulnerabilities. And you're keenly aware that the average cost of a breach keeps climbing, hitting an all-time high of USD 4.35 million in 2022.

But you also know how these risks fit in with broader business crosswinds. You've learned how to work in the face of economic uncertainty, the pressure to do more with less, and a talent shortage that's pushed you to upskill and reskill.

Amidst all these challenges, cybersecurity has taken on a new urgency—even among corporate boards. As a result, CISOs have found wider access and influence in organizations (with some even taking on CIO roles), and many are under pressure to pitch their boards directly for needed cybersecurity investments. So how do you make a strong case?

Your board has the power to set priorities that can put your organization on sound security footing. But just under 2 percent of board members on average have any relevant, recent experience in cybersecurity. And many board members don't feel confident about IT and security oversight, or they have ambivalent views on the board's role regarding security.
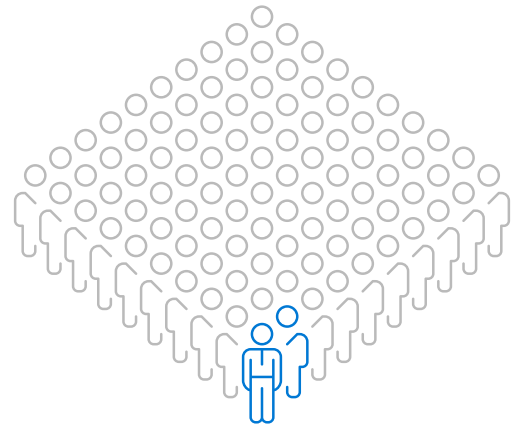
Less than 2 percent of board members on average have any relevant, recent experience in cybersecurity.

The good news is that there's huge potential for getting buy-in on security investments from most boards. The top priorities of a typical board—around risk, reputation, and financial stability—align strongly and organically with successful security outcomes.

If you can connect the dots between those priorities and outcomes, you're well on your way to making a strong, ROI-focused pitch. This guide will help you develop the right context and approach, by showing you how to:

- **Think like a board member**

- **Speak like a board member**

- **Use real-life examples to make risks relatable and relevant**

Think like a board member

Your board may be more attuned to security than you know.

Security is now coming up in board conversations more frequently than ever. Over two-thirds of boards say they now discuss cybersecurity regularly or constantly, and 77 percent of board members believe that cybersecurity is a top priority for their board. And while cybersecurity experience may be rare among board members, overall technology experience has become more common. At leading companies, 79 percent of boards have at least one member with a technology background—and at 72 percent of those companies, technology leaders frequently engage with board directors outside of board meetings.

That's all promising for CISOs. It's still a safe bet, though, to talk less about technology and more about the big picture of enterprise risk and reputation management. Regardless of technical expertise, every board member can comfortably discuss and think about risk, whether that's finding the right level of risk tolerance or evaluating risk management plans.

Cybersecurity is about taking the right risks, not choosing the right technology."

As you're getting into the mindset of your board, start by building consensus around your organization's current state:

- **What do board members consider your most important assets? Is it your customer data, company IP, your brand, or something else?**

- **What do they think are the most threatening risks?**

- **What are the organization's most pressing priorities?**

- **What objectives does the business need to achieve, and how can your security program help enable them?**

Grounding the discussion in these fundamentals creates the right perspective. You can help your board understand that cybersecurity is about taking the right risks, not choosing the right technology.

Speak like a board member

Keep the following ideas in mind as you talk to your board, whether in presentations or less formal communications.

Talk business, not technology.

Use examples and illustrations appropriate for interested business experts, not technical experts. Look to Bloomberg Businessweek or the Wall Street Journal for inspiration around the right level of detail for presenting security concepts. (A recent news story about a breach can also be a great starting point for discussion, as you describe how it might have played out at your own company.) Find someone you trust outside your security organization to give feedback on the complexity of your communications.

Act as an impartial guide and facilitator.

A good security program requires striking a balance—that is, setting an acceptable level of risk to pursue business objectives—and you can help foster that mindset. Demystify tradeoffs for board members and guide them through decisions, rather than prescribing solutions as an authority.

Center on ROI, especially in terms of strategic relevance.

Always show how your security initiatives align with business needs and long-term priorities. Take your organization's top strategic goals—whether that's global expansion, a new customer platform, or digital transformation— and provide the context that demonstrates how the right cybersecurity investments enable and protect those goals.

Demystify tradeoffs for board members and guide them through decisions, rather than prescribing solutions as an authority."

Focus on opportunities, not costs.

Security (and IT more broadly) can suffer from being seen as simply a necessary cost center. Continuing to push your team to find ways to be more proactive can help address that, but you can also champion the role that security can play as a business enabler. CISOs who show how security can drive revenue—for example, by quantifying contract and customer value against spending on controls—will likely find a more receptive audience.

Be ready with metrics and benchmarks.

The business truism that "You can't improve what you can't measure" may have its shortcomings, but carefully curated metrics can still be powerful evidence for boards. Choose metrics that show program maturity and progress over time (such as metrics around security awareness training or the effectiveness of security procedures), as well as how your organization measures up against peers. These maturity metrics will generally be more meaningful (and actionable) to board members than metrics around performance or activity, which can be noisier and require more technical context. Metrics can also help you demonstrate ROI and prudent budgeting. For example, it's a good idea to keep a close eye on how your proportional spend in different security areas tracks with comparable organizations.[1]

Describe risks in ways that make them real.

Focusing too much on fear is typically a dead-end for motivating support and positive action. But the right example or real-life incident can be extremely effective at communicating complexity and risk, without exaggeration or negativity. Look for examples with specifics relevant to your industry or organization, or that illustrate likely scenarios such as insider risk or ransomware. (See the following section for ideas.)

[1] Planning Guide 2023: Security & Risk, Forrester, 2023

Use real-life examples to make risks relatable and relevant

Insider risk and ransomware attacks continue to be prominent threats for many organizations, which makes them useful for illustrating tangible, addressable risk. By walking board members through actual incidents, you can help them better understand these types of attacks, the potential impacts involved, and what kinds of cybersecurity investments might make a difference in similar, future attacks.

Example of a ransomware incident:

LockerGoga attack

March 2019

What happened?

One of the world's largest aluminum companies was <u>attacked with LockerGoga</u>, a form of ransomware. The attack locked the files on thousands of servers and PCs, posting a ransom note on the screens of the corrupted computers. The damage had been set in motion three months earlier when one employee unknowingly opened an infected email from a trusted customer. That allowed hackers to invade the IT infrastructure and covertly plant their virus.

What was the business impact?

All 35,000 employees in the organization across 40 countries were affected. Production lines had stopped at some of its 170 plants. Other facilities were switching from computer to manual operations. The financial impact would eventually approach $71 million.

What could be done differently to prevent similar attacks in the future?

The company's swift and transparent response was <u>widely praised</u>. They chose to pay no ransom, be fully open about the breach, and <u>call on Microsoft's Detection and Response Team</u> (DART), which supports companies under attack. But to prevent similar attacks in the future, DART members outlined how the right combination of people, processes and technology can help. That approach includes implementing multifactor authentication, having a mature update process, backing up data, and increasing security awareness and training among employees.

Making the case

The ideas and examples discussed in this e-book can help you shape your pitch to the board. But ultimately, of course, you'll need to choose the right structure and details based on the investments you need. The following ideas can help as you explore what might work best with your particular board.

- **Don't be afraid to try different approaches.**
  For example, tabletop exercises and other scenario simulations can be a powerful experience for education and engagement, or you might want to bring in an external security expert to speak.

- **Talk to C-suite peers for feedback and support.**
  Your CEO and other fellow executives can be invaluable for insights into particular board members or recurring issues. They can also add weight to your arguments if board members see that leaders across your organization support the investments that you're proposing.

- **Keep communication lines open.**
  Try to build rapport with one or more board members outside of quarterly or annual updates, especially board members who have technology or security experience. They can help advocate for your views when you're not present—and even help you better tailor your pitches.

In the end, CISOs have much cause for confidence right now. More board members than ever are actively seeking guidance on cybersecurity. And many technology developments speak directly to board <u>concerns around cost and ROI</u>—from advances in automation and AI to the potential for integrated security solutions to reduce complexity and cost.

Looking for a place to start?

Use the following discussion guide to think through how SecOps maturity could help you frame a conversation with board members.

How to use SecOps maturity to start a discussion with your board members

Wondering where to begin with board members when talking about cybersecurity risk? Security operations maturity can help give you a framework for more productive discussions.

Take some time to talk through each of the following five areas of SecOps with your security leadership team. If you can better understand where your organization sits on the maturity spectrum for each area, you can identify gaps and strengths— and with that in hand, you can make more specific requests to your board of directors.

For example, in Triage, an organization on the Basic end of the spectrum might not be using automation yet for investigating and remediating high-volume or repetitive incidents. An organization that's Optimized in Triage might use security orchestration, automation, and response (SOAR) services and tools to automate cyberattack prevention and response. By returning to the idea of acceptable risk around different threats, you can help your board better evaluate where your organization should be on that continuum.

Check out the full self-assessment tool for more details.

OPTIMIZED

ADVANCED

BASIC

📋 Triage

How quickly can we assess alerts, set priorities, and route incidents to our security operations center team members to resolve?

Discussion questions for your security leadership team:

Do we have the right approach to prioritizing incidents and threat alerts?	**Should we be using more automation for investigating and remediating high-volume or repetitive incidents?**	**Are we doing enough to manage alert fatigue?**

🔔 Investigation

How quickly can we determine if an alert indicates an actual attack or a false alarm?

Discussion questions for your security leadership team:

How many security tools in total do our analysts use for incident investigation (including vendor products or portals and custom tools or scripts)?	**How do we consolidate and correlate all of our data sources (for example, with a SIEM or other tools)?**	**How do we use detection and investigation tools focused on identity, endpoints, email and data, SaaS apps, or cloud infrastructure?**

🔍 Hunting

How do we search for adversaries that have evaded our primary and automated defenses?

Discussion questions for your security leadership team:

Does proactive threat hunting need to be a bigger part of our security strategy?	**Do we have the right processes and tools to help detect and manage insider threats?**	**Does our hunt team make enough time to refine alerts to increase true positive rates for triage teams?**

Incident management

How do we coordinate response by technical, operations, communications, legal, and governance functions?

Discussion questions for your security leadership team:

Do we have an effective crisis management process for handling major security incidents?	**Does the process involve the right teams, including executive leadership, legal, and communications and public relations?**	**Are we conducting enough regular exercises to practice and refine this process?**

Automation

How are we using automation to save our analysts time, increase response speed, and reduce workloads?

Discussion questions for your security leadership team:

How are we using vendor-provided or vendor-maintained automation to reduce investigation and remediation workload on analysts?

How well can we orchestrate automated actions across different tools?

Are we taking advantage of community-provided automation?

Microsoft Security