Health Sector Coordinating Council
Cybersecurity Working Group

Manage Risks | Monitor Threats | Measure Effectiveness

Health Industry Cybersecurity

A CISO's Primer for Engaging the Board



NOVEMBER 2026

Table of Contents

1. Introduction: Shift from a Technical to a Strategic Conversation 4

2. Understand Your Board 5

- Common Board Committees: 6
- Know Your Board Members Individually 7
- Board Interests by Healthcare and Life Sciences Sector: 7
- Engaging Board Committees 8
- Presenting to the Full Board 9
- NACD's Director's Handbook on Cyber-Risk Oversight 10

3. Prepare Before You Enter the Room 10

- Understand the Threat Landscape 11
- Align Your Approach with Organizational Business Objectives 12
- Be Strategically Aligned and Politically Aware 12
- Know Your Internal Champions 13

4. Building Your Report: Frameworks and Approaches 15

- Board Reports 15
- Structure 16
- Enterprise Risk Management Alignment 17
- Tell a Story: Strategic Risk Management, not just Metrics 17
- Metrics 18
- Frameworks 19
- Risk Management 20
- Consistency 20
- Quantification 21

5. Structuring Board Conversations: Strategy in the Boardroom 21

Clear, Direct, and Confident Communication is Vital 21
Tailor your Message 21
Adapt to the Board's Maturity and Preferences 22
Be an Educator 22
Take an Actionable and Solution-Oriented Approach 24

6. Crisis communication 25

Prepare Before an Incident 25
Communicate Clearly During the Incident 26
Manage Broader Stakeholder Communication 26
Lead Post-Incident Communication and Continuously Improve 27
Crisis Communication Key Takeaway for CISOs 27

7. Conclusion: The CISO as a Strategic Partner 27

8. Appendix: Template for Phased Board Engagement 28

Phase 1: Foundational Engagement and Education (Meetings 1-2) 28
Phase 2: Build a Strategic Partnership; Define Risk Appetite (Meetings 3-4) 29
Phase 3: Ongoing Strategic Oversight and Reporting (Steady-State Cadence) 29

9. Acknowledgments 31

1. Introduction: Shift from a Technical to a Strategic Conversation

In today's digital and AI-driven healthcare and life sciences landscape, cybersecurity is no longer a siloed IT issue. It is a fundamental component of **patient safety, operational resilience, regulatory compliance, and long-term business value**. A Chief Information Security Officer's ability to effectively articulate cyber risk to their Board of Directors is essential to ensure Boards understand business threats and their potential impacts, make informed governance decisions, and support proactive investment in cybersecurity as part of enterprise risk management.

Many CISOs face significant challenges in both communication with the Board and being seen as a strategic partner, for several reasons:

- Insufficient understanding of the Board's role and engagement with Board members
- The outdated view among Board members that cybersecurity is "*just* an IT issue"
- Board members lack the knowledge to ask the right questions or understand the answers
- CISOs do not describe risk in the way the Board looks at other business risks, and instead rely on technical jargon, metrics, and FUD (Fear, Uncertainty, and Doubt)
- Executives prioritize growth and revenue and may see cybersecurity as a competing overhead investment, rather than an enabler of innovation and growth
- CISO communications do not align with business strategy, organizational and capital risks, and investment needs

This primer is designed to equip Chief Information Security Officers (CISOs) with a strategic framework for communicating with their Board of Directors. It enables healthcare and life science CISOs to communicate cyber risk in the language of business, positioning cybersecurity as a key element of sustaining the organization's mission.

> *"One of the biggest shifts in my approach came after recognizing that the Board doesn't react to technical detail, they react to business impact, clarity, and patterns of accountability. Early in my role, I presented risks using technical severity and control maturity. The Board understood the words, but not the weight of the risk. The turning point came during a discussion where a director asked, 'What does this mean for us financially, operationally, and reputationally?' I realized I had been describing security, not risk."*

The HSCC developed this primer in alignment with the S**trategic Objective 5 of the Health Sector Coordinating Council 5-year strategic plan (2024-2029):** *Enhance health sector senior leadership and Board knowledge of cybersecurity and their accountability to create a culture of security within their organizations*. Cybersecurity requires leadership understanding and accountability to foster strong cybersecurity and privacy cultures that permeate from the highest levels within each organization.

Using the framework and principles provided in this primer, the CISO can transform their role to that of a strategic partner, fostering a resilient cybersecurity culture that protects patients, data, and the organization's future.

Throughout this document are text boxes that quote unattributed CISO's sharing with HSCC their lessons learned and good tips from their experiences engaging with their Boards of directors and C-Suite executives.

2. About the Health Sector Coordinating Council Cybersecurity Working Group

The Health Sector Coordinating Council (HSCC) Cybersecurity Working Group (CWG) is an industry-led critical infrastructure advisory council working with the government in a national public-private partnership established under law and executive order. Its more than 500 healthcare providers, pharmaceutical and medical technology manufacturers, payers, health IT companies, public health and government agencies collaborate to identify and mitigate cyber threats to health data and research, systems, manufacturing and patient care. Through direct member engagement and leadership, the CWG develops and publishes free healthcare cybersecurity leading practices and policy recommendations and produces outreach and communications programs emphasizing the imperative that cyber safety is patient safety.

3. Understand Your Board

To effectively engage a Board, it is crucial to understand their responsibilities, primary concerns, and fiduciary obligations. Board members are ultimately accountable for the long-term value and sustainability of the organization through core oversight responsibilities including:

- **Strategic Guidance:** Approving mission-aligned goals (e.g., patient care delivery, research, and development).
- **Risk Oversight:** Identifying, understanding, and mitigating key risks to the business.
- **Executive Leadership Oversight:** Appointing and assessing the CEO and executive team.
- **Financial Stewardship:** Ensuring efficient use of funds and long-term financial sustainability.

Boards are not involved in the day-to-day aspects of running the organization. Following the old adage, "Noses in, fingers out," Boards observe, question, and counsel based on the wisdom of their experience. The Board relies on senior leaders like the CISO to translate complex cyber risk into business-relevant terms. The full Board typically only meets quarterly. Board members receive a Board package prepared by management to review ahead of the Board meeting. This package may contain financial reports, operational performance data, strategic proposals, and risk assessments. Inserting materials into this package is an opportunity for the CISO to educate Board members on key cybersecurity risks at a level of detail that may not be covered during the Board meeting.

> *"The most important factor is to communicate on their terms. How do each of the areas of our framework protect us, and what is the impact if they do not."*

At the meeting, each agenda topic is allotted time. Directors debate and scrutinize management's proposals, asking critical questions to ensure the proposals align with the company's long-term strategy and fiduciary responsibilities. In addition to a succinct presentation, a CISO needs to be prepared to answer questions on the submitted Board package as well as questions based on current events or risks that Board members see at other organizations.

Since Board meetings are of limited duration, the Board may delegate detailed governance work to its functional committees. These committees investigate, deliberate, and then make recommendations to the full Board for final approval.

Common Board Committees:

Committee	Core Responsibility	Activities
Audit Committee (Mandatory for public companies)	Financial Integrity & Risk	Oversees the external auditor, reviews financial statements, and monitors internal controls and compliance. Oversight often includes cybersecurity if there is no Risk or Technology Committee.
Compensation Committee (Mandatory for public companies)	Executive Pay & Incentives	Determines the CEO's and senior executives' salaries, bonuses, stock grants, and severance packages.
Nominating & Governance Committee (Mandatory for public companies)	Board Structure & Ethics	Recommends new Director candidates, leads Board self-evaluations, and oversees corporate governance policies.
Risk Committee (More common in financial institutions)	Enterprise Risk Management	Focuses specifically on identifying and monitoring major enterprise risks, including cyber risk and global economic threats.
Technology Committee (Not common today, but growing in adoption)	Oversight of Technology Strategy	Focuses specifically on identifying and monitoring technology-related opportunities and risk management, such as AI and cybersecurity.

Healthcare organizations may have variations on these committees. For example, “audit and compliance” and “quality and safety” committees may be found in non-profit healthcare systems. Committees are often made up of Board members with relevant experience. An Audit Committee may consist of former Chief Financial Officers (CFOs), public accounting audit partners and persons with similar prior expertise.

It is common for a CISO to present to one or more of the committees responsible for internal control, compliance, and risk in lieu of the full Board itself. Expect the committees to review cybersecurity risk in more detail than the full Board. This can be an opportunity to have more focused and strategic discussions and time allotted for cyber on the agenda.

Given the rise in shareholder litigation and regulatory scrutiny, it is a good practice to work with the Board Secretary and the General Counsel to ensure that Board minutes document that the Board was presented with cyber risk

materials and had a chance to review and question them. This low-cost intervention will strengthen the defensive position if the Board's risk oversight is ever challenged.

Know Your Board Members Individually

Know your Board members individually, their interests and concerns. Understanding their background, field of expertise, and peer networks can strengthen your effectiveness when answering questions or sharing information. Knowing their technical and cyber fluency is key for communicating risk in a way that is readily understood. For example, a Board member who is well versed in cybersecurity would appreciate a more detailed and technical response to their question in comparison to one who is not familiar with cybersecurity at all.

Look up the biographies of your Board members in the organization's Annual Report or LinkedIn. You can use this background to anticipate and answer questions and connect your answers to their background and expertise. For example, knowing that the chair of the Audit Committee is a career CFO indicates you should couch your answers in risk and financial terms. Additionally, many Board members serve on multiple Boards and have held leadership roles at other organizations. Understanding whether those organizations have experienced cybersecurity incidents can provide valuable insight into the perspectives, concerns, and experiences Board members may bring to cybersecurity risk discussions.

Board members usually review presentation materials in advance so they can come prepared with questions or requests for clarification. This makes it crucial that your materials be understandable on their own, i.e., they are going to be read without you being there to explain. When a report highlights deficits or other areas of security concern, it's common for Board members to ask, "What do you need from us?" Because of this, it's important to have a well-considered response ready. Any requests or recommendations you plan to bring forward to the Board should be vetted through the appropriate chain of command before the meeting to ensure alignment and executive support.

> *"I am always there 30 minutes early. It is a good chance to have some informal conversations and build some relationships."*

Board Interests According to Healthcare and Life Sciences Sector:

CISO communications should directly address committee interests, demonstrating how a robust cybersecurity program manages risks and enables the organization to achieve its strategic goals. Each organization is unique. Below are examples of sub-sector common interests to assist in mapping out what may be relevant and of interest to a specific Board or committee.

Sub-Sector	Primary Board Interests
Health Delivery (Not-for-Profit, For-Profit, Government-Owned)	Patient Safety & Health Outcomes, Regulatory Compliance (HIPAA, etc.), Financial Stability, Clinical Innovation,

	Operational Resilience, Reputation and Patient Trust
Health Insurer (Not-for-Profit, For-Profit, Government-Owned)	Member Data Protection (PHI), Regulatory Compliance, Financial Performance, Brand Reputation
Medical Device Manufacturer	Product Security & Patient Safety (FDA regulations), Intellectual Property (IP) Protection, Supply Chain Resilience, Shareholder Value
Pharmaceutical Manufacturer	Intellectual Property (IP) & Clinical Trial Data Security, Regulatory Compliance, Product Integrity & Patient Safety, Shareholder Value
Software Manufacturer	Product Security, Customer Data Protection, IP Protection, Market Competitiveness
Service Provider	Customer Data Security, Service Availability & Resilience, Contractual Obligations, Reputation

Consider how the cybersecurity program connects to and aids these typical areas of focus to the Board by understanding core health entity business objectives such as:

- Providing high quality and innovative patient care and protecting patient safety
- Reducing operational costs while retaining operational reliability and quality
- Enabling entry into new markets and services
- Minimizing the risk of civil and regulatory actions
- Reducing the expected loss from adverse events
- Reducing the actual and expected downtime and affected patients/consumers from security incidents

Showing alignment between cybersecurity program actions and these business objectives builds understanding, a common language, and a strategic relationship between the CISO and the Board.

Engaging Board Committees

In many organizations, theCISO's primary governance interface is the **Audit Committee** or **Audit and Compliance Committee**. These committees are typically focused on regulatory adherence, internal controls, audit findings, and assurance activities. Board members often have backgrounds in highly regulated industries and are fluent in the language of compliance, risk management, and control frameworks.

When engaging these committees, CISOs should emphasize:

- How the program engages with business initiatives

- Operational, regulatory, and legal risks
- Program adherence to a recognized framework, such as the National Institute of Standards and Technology's Cybersecurity Framework
- Results of audits and assessments of control effectiveness and gaps
- Remediation priorities, progress, and obstacles
- Independent validation and assurance activities

Discussions are generally more detailed and operational than with the full Board, and there is some tolerance for technical depth if it remains tied to risk and accountability. For a new CISO, understanding the committee's historical concerns, recurring findings, and prior reporting formats can significantly improve credibility and efficiency.

This forum also provides an opportunity to build trust through consistency and follow-through, as Audit Committees tend to value discipline, predictability, and measurable progress.

Presenting to the Full Board

Presentations to the full Board require a different approach. Time may be limited; they may have less context and knowledge; attention is fragmented, and senior leadership—often including the CEO and Board Chair—are present. The expectation is to articulate priorities with confidence.

Full Board discussions typically focus on:

- The most significant cyber risks
- Program strategy, key priorities, and significant investments
- How program activities are benchmarked to industry peers
- The organization's readiness and resilience
- Clear plans and timelines for risk reduction
- How cyber-strategy aligns with overall risk appetite

In the Board setting, the CISO is not seeking approval for every action but reporting on progress, outcomes, and value creation.

The implicit question from the Board is: How well is management addressing this risk? Do they *understand the risk, how are they addressing it, what obstacles are in the way, and how quickly will we meet our goal?*

Understanding how the Board prefers to consume information is essential. Many organizations rely on executives such as the CEO, CFO, or corporate secretary to manage Board interactions. Engaging these leaders, as well as the CIO, Chief Legal Officer, and head of Internal Audit in advance of each Board meeting can provide insight into preferred formats, sensitivities, and emerging priorities—as well as identify topics that require careful framing and potential questions Directors may ask.

Done well, full Board engagements reinforce the CISO's role as a business leader and risk advisor, not merely a technical expert.

NACD's Director's Handbook on Cyber-Risk Oversight

In recent years, there has been an increased interest in what Boards are doing to understand and help govern cybersecurity risks. Several notable breaches have led shareholders, the SEC, and other interested parties to ask what more a Board should be doing to ensure that cyber risks are being appropriately managed by the Board and throughout the organization.

To help establish common industry practices and expectations for Board governance, the National Association of Corporate Directors (NACD) teamed with the Internet Security Alliance (ISA) to develop guidance. It is helpful for CISOs to be aware of these principles, as they will be of aid in having more strategic conversations with the Board and its committees. The "NACD/ISA "Director's Handbook on Cyber-Risk Oversight" (5th edition, May 2026) outlines six fundamental principles that should guide Board-level engagement on cybersecurity. CISOs should be prepared to address each of these principles in their overall approach with the Board, including in their communications.

The Six NACD Principles:

1. Cybersecurity as a Strategic Risk: Boards should view cybersecurity not as an IT problem, but as a core enterprise risk that impacts long-term value creation. Your role is to help them understand this connection.
2. Legal and Disclosure Implications: Directors need to be aware of the evolving legal and regulatory landscape, including breach notification requirements and potential liabilities. Provide regular updates on SEC, HIPAA, GDPR, state laws, and FDA cybersecurity requirements.
3. Board Oversight Structure and Access to Expertise: The Board should have access to cybersecurity expertise, whether through its members or external advisors. Offer to provide regular briefings and educational sessions.
4. An Enterprise Framework for Managing Cyber Risk: Management is expected to establish a comprehensive, enterprise-wide framework for managing cyber risk, with adequate staffing and budget. The NIST Cybersecurity Framework can serve as a foundation.
5. Cybersecurity Measurement and Reporting: Board discussions should include quantifiable metrics on financial exposure to cyber risks and the effectiveness of mitigation strategies. This is an opportunity to tie cyber risk into the organization's enterprise risk management program.
6. Encourage Systemic Resilience and Collaboration: In an interconnected healthcare ecosystem, Boards should encourage collaboration with industry peers and government agencies to enhance collective resilience. Highlight your organization's participation in the Health Information Sharing and Analysis Center (Health-ISAC) and other collaborative efforts.

4. Prepare Before You Enter the Room

Effective engagement with the Board begins before the meeting. Preparation is not only about building materials, but about aligning cybersecurity with business priorities, organizational dynamics, and Board expectations.

"They will read you more than they will read your slides."

"CISOs who understand their audience, anticipate questions, and align messaging across their executive suite are better positioned to drive a meaningful dialogue and alignment with their Board. This preparation builds trust, and enables more informed decision-making in the Boardroom."

Advance preparation should also include coordination with C-suite executives, to show broad business ownership and alignment. Indications that the CISO is "alone on an island" without engagement or accountability from others is a red flag to a Board.

Understand the Threat Landscape

A CISO must be informed about emerging threats, industry hot topics, and active attack trends— and be ready to explain why each is or is not relevant to the organization. Board members tend to be well read, and you should be ready to speak to a cybersecurity story in today's key periodicals, such as the *Wall Street Journal*. Align your presentation to the threats that may impact the company from achieving their corporate objectives, not just your team's goals. Because the nature and volume of cyberattacks shift over time, having not just an understanding of these patterns, but being able to speak to the Board on what is relevant and what does not carry associated risk to the organization is essential. This awareness ensures that future security strategies and investments align with the threats most likely to impact the organization and build credibility on where valuable attention should be given.

Healthcare cybersecurity threat information is available from government agencies and industry associations including:

- Health Information Sharing and Analysis Center (Health-ISAC)
- Department of Health and Human Services
- Health Sector Coordinating Council Cyber Working Group
- American Hospital Association and other trade groups to which your organization belongs
- Cybersecurity & Infrastructure Security Agency
- European Union Agency for Cybersecurity
- MS-ISAC (https://www.cisecurity.org/ms-isac)
- FBI Cyber Alerts (https://www.fbi.gov/investigate/cyber/alerts)

For more information about information sharing organizations, their resources and terms of engagement, see the HSCC's Health Industry Cybersecurity Matrix of Information Sharing Organization (HISC-MISO).

While HSCC does not endorse any particular vendors, well known private sector incident response and threat intelligence firms publish annual cybersecurity threat landscape reports, such as:

- Verizon - Data Breach Investigations Report (DBIR)
- Microsoft – Digital Defense Report
- Mandiant (Google Cloud) – M-Trends Report

- IBM – Cost of a Data Breach Report
- CrowdStrike – Global Threat Report and, Sophos, Trend Micro, Cisco, RSM, Palo Alto Networks (Unit 42)

Also consider subscribing to credible news outlets that the organization's executive team and Board members are likely to have in their news feeds or common outlets that they may be following, such as publications like:

- Wall Street Journal
- Forbes
- New York Times
- Becker's Hospital Review
- Modern Healthcare
- Financial Times
- The Economist
- Bloomberg
- Harvard Business Review

Being aware of current events and news before you receive a panicked call from a Board member or Executive will build credibility and prepare you to answer questions you may receive while meeting with the Board in an official meeting. You can quickly address why the current event may or may not be relevant and your strategy to address if needed.

In addition to published reports and threat intelligence sources, regular engagement with industry peers through the Health-ISAC and HSCC CWG can provide valuable context on emerging threats, common challenges, and effective mitigation strategies. Board members and executive leadership are often interested not only in the threats facing the organization, but also in how peer organizations are responding.

Alignment of Business Objectives to Cyber Benchmarking with Competitors

There are several ways to find out where your organization is positioned in the market. Your annual report and public website are good starting points. For a broader context, search online business journals for stories about your organization. Understand what your executives are saying, as well as your competitors and industry leaders. Consider reaching out to your colleagues in 'competitive intelligence' if that function exists in your organization. This function may also be part of another marketing or finance function, so it is best to ask whether this function exists elsewhere. Ask for prior external audit reports that may exist that compare your organization with others in your sector. Finally, for information security specific information, look for prior internal or external audit reports that benchmark your security program with that of other companies in your sector or leading practices across industries. Together, these inputs help you identify gaps and focus your efforts on what matters most to the business.

Be Strategically Aligned and Politically Aware

As a CISO, focus on business impact. Questions you could ask:

- What are the CEO's top three priorities this year?

- How is senior executive performance measured (e.g., stock price, revenue)?
- Where is the company most financially and risk-exposed?
- What cyber initiatives have sensitive policy, legal, compliance, or political implications (acquisitions, layoffs, AI, cloud computing, etc.)
- Where could negative cybersecurity events most impact our goals?
- How are our actions reducing the risk of negative impacts?

The CISO's messaging should clearly map directly to these business priorities. For example, rather than saying, "We have a vulnerability management maturity gap" offer, "Attacks using ransomware have shut down IT systems at dozens of hospitals, significantly impacting patients and clinicians, as well as revenue and reputation. As a result, we are focused on remediating found vulnerabilities that could be exploited in a ransomware attack". This second statement conveys urgency, shows direct patient care and revenue impact, and speaks the language of business.

Regardless of your prior experiences, as the CISO you are a business executive accountable to the security and resiliency of the organization's digital and operational assets. You should evaluate security risks in the context of business objectives.

While a CISO needs to be clear and direct regarding risk, that message must be delivered with dispassionate analysis. For example, "As we expand AI adoption, complexity has increased. While controls are in place, additional automation could increase operational risk. We have/are evaluating solutions to address this, and the key to success is for the security team to be engaged from the start on new initiatives, so controls are baked in."

Understand the politics in your organization. Make sure your Board presentation has been presented to your CEO and broader executive team and vetted by Legal prior to the actual Board presentation. Never present to the CEO or Board without your direct manager's visibility.

If you are presenting metrics, have a baseline of what you are comparing and why one metric is good or bad. If a baseline has never been established, state that.

As you present, maintain situational awareness. Look for body language. Listen for who is and who is not asking questions. Are there questions behind the questions that need to be surfaced? Are Board members asking operational questions? These could be signaling that there are unspoken concerns.

As CISO, you are the organization's strategic risk advisor. Signs that you are making progress will be a shift in how the Board and fellow executives ask questions to better understand and manage cyber risks. You are not just pulling the cyber alarm; you are advancing risk awareness; protecting executive trust; and most importantly enabling the business.

Know Your Internal Champions

Effective Board reporting is rarely a solo effort. CISOs who succeed understand the importance of cultivating strong relationships with key collaborators across the organization; particularly those who already have the Board's trust. Finance, legal, internal audit, compliance, enterprise risk management, and operations leaders can be powerful allies in shaping a coherent and credible narrative about cyber risk. Aligning messaging with these stakeholders ensures consistency, avoids surprises in the Boardroom, and positions cybersecurity not as a standalone technical issue, but as an integrated component of enterprise risk, financial resilience, and regulatory accountability.

"I never brief the Board until Legal, Finance, Operations, and IT are aligned on a single, coherent narrative – conflicting messages erode trust faster than an incident itself."

Equally important is identifying and nurturing internal champions who can reinforce your message at the Board level. This may include the CFO contextualizing cyber investments in business terms, the Chief Risk Officer framing cyber threats alongside other top enterprise risks, or the General Counsel articulating regulatory and legal exposure. You should proactively brief these leaders, share talking points, and test key messages before formal Board interactions. When trusted executives echo and support your perspective, Board discussions become more strategic, credibility increases, and security initiatives are more likely to gain sustained support and funding.

Another exercise is to map unspoken sensitivities, such as those in the following table:

Executive	Common Sensitivity
Chief Executive Officer	Reputational, operational disruption
Chief Financial Officer	Cost, financial exposure
Chief Compliance Officer	Regulatory exposure, reputation
Chief Information Officer	Operational disruption
Internal Audit	Audit effectiveness and independence
Chief Operations Officer	Operational downtime
Chief Medical Officer, Chief Nursing Officer and Chief Medical Information Officer	Disruption to clinical care
Board	Strategic risk and public impact

Organizations of any size can have political considerations. As a CISO, you need to understand these – knowing who is influential and how. Consider, for example, who influences the CEO most, who seems to drive investment decisions, who has the Board's trust?

When prepping your materials for the Board, take a moment to ask, "Who could feel exposed or surprised by this information?" Meet your fellow executive presenters in advance. Do not surprise executives in front of the Board. Brief the CEO prior to any Board meetings. Socialize risk with the CIO/CTO first. Align with the CFO on financial impact and with the CCO on regulatory risk and impact

The language in the Boardroom is simple: "Management and security leadership have jointly identified…." This builds trust and credibility.

Having said the above, the message the CISO gives to the Board should match the internal assessments and metrics. Coordination with business leaders to avoid surprises does not mean "softening" or "sugar-coating" the message. This is where relationships and credibility across the C-suite come into play.

5. Building Your Report: Frameworks and Approaches

There is no one size fits-all approach to cybersecurity reporting at the Board level. Effective communication requires selecting frameworks, metrics, and reporting structures that align with the organization's business objectives, overall risk appetite, enterprise risk management approach, and Board expectations.

> *"Your job as a CISO is to tailor the cybersecurity risk to the cybersecurity risk appetite of your organization."*

Board Reports

Board reports should be customized to the communication preferences and expectations of the Board. Some Boards may expect dashboards of metrics while others will look for more narrative formats. Ideally, the CISO report should align with reporting from Enterprise Risk Management (ERM), to demonstrate that cyber is another element of business risk, not a one-off.

If your organization does not have ERM reporting, you can develop your Board report and strategize your communication plan by asking other executives to share their reports and look over prior reports from others, like the CEO, COO, CCO, and CFO. Note the types of issues covered, the layouts and graphics used, and the frameworks or metrics used, and their level of detail in communication. Also make note of where content is found; is it primarily in the appendix of the Board report or are there many examples of content heavy slide decks? These are great sources for learning what the Board expects.

> *"For Boards – metrics are not to catalog effort, it's to understand exposure, trajectory, and consequence. They want to know whether a risk is increasing or decreasing, whether controls are effective, and whether the organization can limit damage when prevention fails."*

Board reports are often composed of two parts: the pre-read and the presentation. A pre-read is typically distributed ahead of the Board meeting in a Board packet. The pre-read may contain an overview of the organization's risk

posture, business justification for spending requests that exceed the CFOs authority, updates on current events, educational content, and other material.

Depending on the Board's culture, Board members will review prior to the meeting and develop questions to ask during the Board meeting. The Board presentation is a more focused set of materials that you intend to share in the Board or committee meeting. The presentation itself may also commonly be distributed ahead of time; however, it is limited to what you will be presenting in the Board meeting.

Structure

Given the uniqueness of each healthcare organization, there is no universal template for Board reporting. That said, there are some common elements that should be considered:

Top enterprise cybersecurity risks: These are often described in the form of a risk register and ranked. A brief description of the risk should be provided, as well as the risk treatment being applied to the risk (e.g., is the risk being transferred through insurance or changes in commercial agreements). This is where you are showing what is being done to address risks to the company. Be prepared to explain risk and why its treatment is appropriate and what else may have been considered. This is a form of Board education in addition to program accountability.

Emerging Issues: Help explain to the Board what your threat intelligence indicates are rising concerns and why. This is not a "reporting of the news" but is focused on why this threat is a concern to the company and what is being done in response (e.g., acting, monitoring, or staying on course). A current example would be the impact the rapid adoption of agentic and frontier AI models have on vulnerability management.

Security events: Review security events experienced in the last quarter directly or through third parties. Identify what occurred and any outcomes, and what was learned as a result, including changes to telemetry, controls, or programs. This is also a good place to describe what is needed to remain vigilant and resilient: purple teaming, tabletops, external pen tests, incident response planning, etc.

Current and trending metrics: Report on the indicators of a healthy security program. These should help explain how well the strategy and tactics are working. These should not be simply measures of activity, but rather effectiveness. Describe what was implemented in the prior quarter; what happened as a result that improved the security posture of the organization. Use ratios to show relative performance. Relate these measures back to the risks you are concerned with managing. For example, don't simply report the number of scans completed or the number of patches applied, but express it as a coverage ratio (percentage of assets) and whether that is improving over time. For example, report improvements in the velocity of patching – are patches being applied faster?

Investments: Don't simply go with budget requests. Demonstrate what the company has received from prior investments in security. Show the Board that the security organization is a good steward of company resources. Show industry benchmarks (if you have them) that demonstrate value – for example, show what is being achieved as a percentage of revenues. Show how the budget is being directed to protect key revenue streams and the mission of the company. If there is a significant investment required, coordinate with the CFO to describe the investment in financial terms that the Board understands. Describe the return on investment over a period and how that investment will be evaluated.

Enterprise Risk Management Alignment

Engage with Board members to understand their priorities (e.g. patient safety, operational uptime, regulatory compliance) and adjust your communication framework accordingly. For example, a hospital system might worry about how cyber threats could impact patient care delivery, whereas a pharmaceutical company's Board may be concerned with protection of intellectual property. The key is to frame cybersecurity in terms of business impact specific to your healthcare context, making it clear why security matters for mission-critical outcomes (patient safety, trust, financial stability). This tailored approach ensures the Board sees cybersecurity not as a technical issue, but as an integral business risk that varies by organization.

> *"I realized I needed to be laser-focused on the cyber risks most likely to impact business continuity and our role in public health – not theoretical or long-term maturity discussions."*

> *"It's important to gain the confidence of the Board by explaining how top cyber risks can impact our business goals and what we are doing to manage those risks. Discussing cyber risks without connecting them to business impact is less likely to resonate with Board members who are focused on helping the organization achieve its strategic objectives"*

Board materials should mesh with the organization's overall risk management framework, reinforcing that cybersecurity is managed just like other enterprise risks.

Check that the approach to categorize and discuss cyber risks is consistent with the Enterprise Risk Management Plan (ERMP) and the language the rest of the business uses. In practice, this means mapping cyber threats to the same risk categories the Board already understands – financial, operational, reputational, compliance, etc. For instance, if the ERMP evaluates risks in terms of impact and likelihood, your cyber risk updates should use similar scales and terminology.

It's often effective to integrate cybersecurity risks into the corporate risk register and profiles. NIST's guidance (IR 8286) advises incorporating cyber risk data into ERM processes for consistency. By aligning with ERMP, you ensure that cyber risk is prioritized alongside other top risks, and you help the Board see a unified risk picture. You might even present a consolidated risk dashboard that shows the interrelationship between cybersecurity risk and existing financial and operational risk metrics, highlighting where cyber threats could disrupt critical healthcare services or finances. This alignment builds credibility – it shows that the security program supports the enterprise's strategic risk objectives rather than using a standalone or siloed model.

Tell a Story: Strategic Risk Management, not just Metrics

Articulate how Cybersecurity risks impact patient safety, service continuity, financial performance, and regulatory compliance. Deliver a message that resonates and provides them with actionable and solution-oriented information that can assist in building relationships and trust.

Use stories to communicate risk identification and management. It is better to use an illustration of how the security program is helping ensure reliable clinical operations than to simply show a table of figures. Metrics are important, but they are much more powerful when connected to narrative.

"Another pivotal moment came during a real-world incident involving a third party dependance. Although the event was contained quickly, the Board's first questions were about material exposure, regulatory implications, and recovery time – not the technical cause. That made it clear that I needed to regularly frame cyber risk in the same language used for enterprise risk: likelihood, impact, financial exposure, and dependency mapping. Using the FAIR Risk Ontology addressed this issue."

Regardless, narratives and metrics should clearly articulate how your cybersecurity program helps ensure patient safety, service continuity, financial performance, and regulatory compliance. Show a clear connection between the actions you are taking and the results you are seeing. For example, rather than talking about the number of systems that have been vulnerability scanned, or the number of systems patched, tell a story about its importance and the improvement results in terms of risk reduction. How does it make the organization more resilient, and the patients better cared for?

Use stories to illustrate innovation in the security program. What has your organization learned or improvements made over time? Show how your teams collaborate across the business – working with Finance to lessen the cyber insurance costs, working with IT to better support end users' productivity, or partnering with clinicians to rapidly restore a clinical system or prevent its downtime. Let the Board see that cybersecurity is an enabling partner in the organization.

Metrics

Building on what was described above, Board members respond best to clear, outcome-oriented metrics rather than deep technical details. Identify a handful of cybersecurity Key Risk Indicators (KRIs) that speak to the organization's financial, operational, and reputational risks. Each metric should connect to what the Board cares about. If operational continuity is a concern, highlight metrics like system downtime due to cyber events or percentage of mission-critical devices secured. If financial risk is key, emphasize potential cost avoided by risk mitigations or cyber insurance status.

It often helps to present these metrics visually, so consider using simple charts or heatmaps in your Board reporting. A common approach is a risk heat map plotting likelihood and impact of top cyber risks (with high-risk items in red); this gives Directors an instantaneous view of your risk landscape. You can also use trend graphs or dashboards to show progress over time, such as improvement in incident response over the last year, or control maturity rising according to a framework scale. Dashboards that map security posture to business goals are particularly effective: for example, a dial chart showing cyber risk posture versus the company's risk appetite, or a bar graph comparing cybersecurity readiness this quarter to last. Always explain why each metric matters to make the business benefit explicit. By focusing on optimal and meaningful metrics linked to enterprise risks, you enable the Board to grasp cybersecurity performance in terms of impact on financial performance, operational resilience, and reputation.

Boards are accustomed to financial reports and dashboards and, out of a lack of understanding may ask for the same from the CISO. Focus on the story you need the Board to understand, and use metrics to support it (but keep them in an appendix). For example, trending of results from phishing simulations is not a Board-level topic, what matters to a Board is "Our workforce risk, and what we are doing about it," which can be assessed based on phishing test results, failed logons, attempts to visit blocked malicious sites, and a dozen other metrics. Use metrics to tell your story, not fill in a dashboard.

Frameworks

Adopting a well-known security framework can lend structure and credibility to your Board reporting. There are several common ones, each with different strengths. It's important to choose the framework that best fits your organization and your Board preference. This table summarizes how commonly-used cybersecurity risk frameworks support Board-level cyber risk oversight across public, private, and hospital-based healthcare organizations.

> *"I chose NIST CSF because it is widely adaptable, easily understood, and allows benchmark comparison to industry peers."*

> *"I chose HITRUST because it's a requirement with many of our third parties but also prescriptive which enables me to clearly articulate progress to our Board year over year."*

> *"My Board was composed of cyber novices and rather than focusing on frameworks, I drove conversations based on business risk. This helped them understand how cybersecurity impact patient safety, financials, compliance, and other factors they understood."*

Framework	Board Maturity	Perspective it provides the Board
NIST CSF 2.0	All levels	Enterprise cyber risk structure with a dedicated GOVERN function; Simple framework; widely adopted framework
NACD Cyber-Risk Oversight Framework	All levels	Director-designed framework focused on fiduciary duty, risk appetite, materiality, oversight cadence, and management accountability
COSO ERM Framework	Med-High	Integrates cyber risk with enterprise risk categories such as clinical quality, financial, regulatory, and reputational risk
ISO/IEC 27001	Medium	Externally defensible certification that provides assurance of information security management maturity; more common outside of the US
FAIR	High	Quantifies cyber risk in financial terms to support materiality assessment, investment decisions, and risk discussions

		Ideal for Boards that make decisions about cyber spend; not control based
NIST IR 8286	High	Provides specific guidance for integrating cyber risk into enterprise risk management and Board reporting

Whichever framework you pick, ensure it is aligned with the enterprise's risk management approach (for example, if your company uses COSO ERM for overall risk, tie your framework of choice into those principles). Then, use it consistently as the basis for your Board reports, so the Board gets a familiar, structured view of your program's status.

Risk Management

Beyond the high-level framework, present a program management view that links security activities and resources to the top risks. Boards want to see not just what the risks are, but what you're doing about them and that they are within the risk appetite of the organization. Consider including a brief overview of your security strategy and key initiatives, framed in business terms. For instance, you might communicate: "To address our top risk of ransomware (which could halt hospital operations), we've prioritized projects in network segmentation and backup system upgrades this quarter." This shows how your team and budget are allocated to mitigate the risks that matter most.

Some CISOs use a simple table or dashboard to show the top 3–5 risks and the major security initiatives or investments addressing each. By doing so, you connect the dots between resource deployment and risk reduction. This programmatic view, grounded in a chosen framework, demonstrates a methodical approach – the Board will see that you have a clear method (framework), a plan of action, and alignment with enterprise priorities.

Consistency

Once you've established a reporting structure, metrics, and narratives that work, stick with it. Consistency is key for effective Board communication. Board members may only deep dive into cybersecurity a few times a year, so it's crucial that each report follows a familiar format and tracks the same or comparable metrics. This allows the Board to easily compare status to past reports and see trends (improving, worsening, or stable) in your cybersecurity posture.

Avoid the temptation to overhaul your reporting approach frequently; don't switch your framework or Key Risk Indicators (KRIs) every meeting. Sudden changes in how you measure or present performance can confuse Directors and erode confidence. Changing your strategy or metrics without good reason can look like you're "moving the goal post" on what success looks like.

If you do need to refine metrics or strategy (perhaps due to a major shift in the threat landscape or business priorities), explain the change and maintain as much continuity as possible with previous reporting. For example, provide prior reporting format in an appendix, so prior comparisons are still available. The goal is to establish a long-

term narrative: using the same core KRIs and risk categories each time, show the Board how your cybersecurity program is evolving and improving against the set goals. Consistent reporting builds trust. Over time; the Board will come to understand the security dashboard you present and gain confidence in both the metrics and the management behind them.

Quantification

The FAIR methodology and similar models suggest ways to quantify the costs of cyber risks. This approach is far from perfect, and most organizations lack the needed data, but quantification of risk in dollars is the language of business and should be the CISO's goal. Take the first steps down this path, improve incrementally, and strive to present cybersecurity risk in dollars, so associated investments and risk reduction can be compared.

6. Structuring Board Conversations: Strategy in the Boardroom

Clear, Direct, and Confident Communication is Vital

When talking to the Board about cybersecurity, use direct and non-jargoned language. Board members are focused on patient care, safety, regulatory obligations, financial stewardship, and community trust. Technical terms and industry jargon generally do not resonate, and worse, make it harder for you to make your points to the Board. Illustrate cyber risks through impact on issues like delayed surgeries, hospital diversions, unavailable electronic health records, or patient data exposure. Frame cyber issues and risks in terms that relate to the ability to conduct clinical or business operations and the impact on patient safety and revenue.

> *"The Board can handle the truth so give it to them. Tell them what your weak areas are, how that will impact your business goals and tell them what you plan to do about it. They will want to know how we are doing compared to our industry peers so be prepared with that data."*

> *"Tell them what they NEED to know, not all the things you want them to know."*

Tailor your Message

Every Board is different as well as individual Director's understanding of cybersecurity. CISOs should take the time to understand who is in the room, what they already know, what level of detail will help them make an informed decision, and be able to translate cyber issues and risks into business impact.

> *"I have seen Boards glaze over serious issues when conversations are filled with technical language and acronyms; their attention shifts from the risk itself to understanding the terminology, which creates confusion and leads to either missed signals about the real operational exposure or delayed decision-making."*

Some Directors may have strong backgrounds in technology, risk, or cybersecurity and are more comfortable with technical terms, while others may be newer to cybersecurity topics and need more context before getting into the issue. While there may be one or two tech-savvy directors, CISOs should not speak one language to one or two directors and leave the others in the dark. Meet the Board at the level of the lowest common denominator of technical knowledge. Board members will appreciate you making it easier for them to understand the issues if they lack a technical background. The level of detail and explanation should match the overall Board's expertise.

Always be thinking about how to relate your work to the decisions the Board is responsible for making. This builds credibility, trust, and engagement.

When CISOs take the time to match their presentation to the background of the Board, members are more likely to ask questions, engage in thoughtful discussion, and provide meaningful insight. Ensure that every Board member leaves the room with a clear understanding of how cyber resilience supports safe, and reliable care for the communities they serve.

Adapt to the Board's Maturity and Preferences

A critical mindset for any CISO entering a new organization is to focus on the present to ensure success. What worked with a prior Board may not translate directly to the next. Every organization has a distinct culture, risk tolerance, and level of cyber fluency shaped by its industry, leadership, regulatory exposure, and history.

> *"One of the most important lessons I learned early in my first CISO role was that the Board does not view a new CISO as starting with a clean slate. Instead, they see you as a continuation of the existing cybersecurity program. You inherit the strategy, roadmap, investments, and team that came before you."*

Boards vary significantly in their cybersecurity maturity. More mature Boards typically expect structured metrics, trend analysis, benchmarking, financial quantification, and forward-looking indicators that connect cyber risk to enterprise outcomes. They are comfortable discussing risk appetite, control effectiveness, and investment trade-offs, and they often expect the CISO to speak concisely in the language of business risk. A majority of Boards are less mature and may require a more educational approach. In these settings, narrative explanations, visual summaries, and clear analogies can be more effective than dashboards of metrics.

The CISO's role expands beyond reporting to that of an educator, including building foundational understanding—what the risk is, why it matters, and how management is addressing it. Over time, consistent and well-framed communication can help raise the Board's overall cyber maturity.

Be an Educator

Ensure every Board member—regardless of technical background—can understand the narrative and understand the status of the organization's cybersecurity program. Leaning into the educator's role means taking ownership of the Board's understanding. In practice, that starts with how you structure your presentation and approach.

A clear agenda that can speak to all levels of cybersecurity understanding, lowers cognitive demand and helps Board members track the conversation even if they're not adept at understanding the day-to-day cybersecurity operations.

An educator also narrates transitions (e.g., "Now that we've covered how we detect issues, let's talk about how quickly we can recover"), so it feels like a coherent walkthrough rather than a series of disconnected updates.

As an educator be prepared to be faced with questions such as "Are we secure?" and treat that as an opportunity to further engage the Board with your strategy towards organizational risk.

> *"I use phrases such as, "the key takeaway is" or the "one thing to remember is" to close important commentary and put emphasis on what you want the Board to be focused on."*

The best Board educators make complex topics simple by using repeatable presentation patterns and strategic frameworks. Being consistent from meeting to meeting allows for a common rapport to develop and allows the focus to be on the content and conversation and not on navigating new layouts. This also allows you to use comparisons over time – illustrating where you were and where you are today.

> *"My most memorable Board interaction was having a deep fake video created of me "presenting to the Board on AI risks". Once the video was done, I explained that I had nothing to do with creating the video. It was a way to educate our Board on the real risks of AI."*

State clearly what you know and what you are still investigating. If it's something you know to be true, share the evidence, so the Board learns how to validate security claims. If it's uncertain, explain why and what you are doing to learn more. This helps them understand how we build evidence and confidence in our assessment of risk. Boards respond well when you're clear on confidence levels without sounding like an alarmist or overly reassuring.

As an educator, see questions as an opportunity to deepen Board understanding. You want the Board to feel comfortable asking questions and use it as an opportunity to clarify or reinforce concepts and program elements. If the questions require more depth and time, note it, and ask the Board how they'd like to address those further questions. This may be through a committee, in a document or in an additional Board meeting.

When you see confusion or pause (e.g., silence after a dense slide, repeated questions, people asking about a jargon you used), treat it as a signal to re-teach, not to push forward. A simple "Let me restate the takeaway" is often the difference between a Board that nods politely and a Board that genuinely understands.

Be consistent over time. Boards build cyber fluency with each meeting, so you want stable definitions, categories, and "what good looks like" targets. If you change labels, metrics, or framing every quarter, Board members will spend their limited time reorienting instead of understanding and focusing on the presentation of key points.

Ideas to consider – will the CEO allow you to add a "one-pager" on a cybersecurity topic to each Board binder, separate from your update and purely for Board education? Even better, can you hold a high-level tabletop exercise to simulate a cyber event as a Board education event?

Take an Actionable and Solution-Oriented Approach

Effective Board engagement is a sustained dialogue that builds over time. Communication with the Board should be tied to actions you are taking and represent what you are planning to accomplish regarding the issues you have or will be raising.

> *"You cannot drop problems/issues without providing your resolution or plans for resolution."*

> *"Don't overwhelm the Board with detail—give them clarity, not complexity. And never walk into the Boardroom with a problem unless you're also bringing a solution."*

This communication can be more effective if you have been building a base of education and awareness over time that is sensitive to and has built the cybersecurity maturity of the Board. One way of ensuring this groundwork is in place is to take a phased approach to Board communications.

A phased approach allows you to first establish a common language and understanding, then move to strategic alignment, and finally settle into a rhythm of continuous oversight.

If you have a Board that has little background or exposure to cybersecurity, it is helpful to have an approach that builds a foundational understanding that ties cybersecurity to the business objectives and mission of the organization. Do not dive right into security technologies and threats. Set the strategic context for the role that you and your organization play in managing a class of risk to the business. Explain how your team protects the mission and ensures resilient operations. Explain risk management and how you try to eliminate, mitigate, transfer, and accept risks. Give some examples of each, like mitigating risks with patch management, or transferring risks with cyber insurance. Talk about the security organization and various roles exist to protect the business. Then begin to take an incremental approach to talking about the threat landscape, and what controls are being applied to those threats. Be very clear with tying threats and controls and explaining how they work to mitigate risks. Be careful to take this in small increments that match the learning capacity of the Board.

If you have a Board that has some experience and expertise with cybersecurity, understand how that expertise is distributed. If there are only a few "experts", then have a plan to address their needs, but also to help those with less experience to learn. Often Boards with a few experts will defer to those individuals, and that can limit the discussion and feedback from the Board and limit your influence on only a few members. Think about developing the Board's overall experience level, with deeper discussions with a few more expert members offline and targeted learning for more novice members. With more experienced Boards, as you begin talking with them, be prepared to speak to your observations of the existing state of security in the organization and what most concerns you as CISO. Expect that this will be followed up with a request to brief them on your plan to address findings.

An example of a phased approach can be found in the appendix.

7. Crisis communication

Effective communication in times of crisis is a critical component of security leadership, not a downstream tactical activity. The CISO plays an important role in communicating with the Board during a cyber incident, or any other critical security event, but typically does so as part of a broader executive response led by the CEO, General Counsel, and Corporate Communications. The ability to communicate clearly and credibly with the Board is built well before a crisis occurs. Strong Board relationships, shared expectations, and an agreed governance model allow CISOs to support executive leadership and help guide Directors through high-stress, high-impact situations with confidence. In practice, a CISO's effectiveness during a crisis reflects the trust, familiarity, and communication discipline established long in advance.

CISOs who communicate regularly, concisely, and in business-relevant terms reduce both variables. When a crisis arises, the Board already understands the organization's risk posture, your leadership style, and how decisions are made. This allows the conversation to focus on outcomes, tradeoffs, and direction rather than credibility or surprise. While the executive team drives the overall response, the CISO can then focus on providing informed recommendations, risk insights, and technical context that support effective decision-making.

> *"The Board wants confidence that they will be informed on the right situations and that there are the right leaders managing the situation to reduce the impact to the company. Credibility and confidence from the Board is built over time through consistent and clear communications. You must be the calm amongst the storm of any incident."*

Prepare Before an Incident

Crisis communication starts with transparency about preparedness. Boards should have a clear, pre-incident understanding of the organization's current security posture, incident response maturity, and historical performance. Effective CISOs routinely brief the Board on recent incidents and near misses, what was learned from them, and how those lessons have translated into concrete improvements. This demonstrates competence, accountability, and continuous learning. These qualities matter far more during a crisis than technical detail.

Equally important is establishing the framework for incident communication ahead of time. CISOs should ensure there is clarity on who communicates to whom during an incident. This should tie to the organization's emergency preparedness efforts and include how and when the Board is engaged. Preparation should also include business continuity and disaster recovery planning, ensuring that critical operations can be sustained or restored while incident response and communication activities are underway. This typically involves leveraging an incident or emergency command center structure, with defined escalation thresholds, decision authorities, and communication roles. When expectations are set in advance, frequency of updates, level of detail, and channels for communication, the organization avoids confusion, duplication, and uncoordinated messaging when time pressure is highest. You should be aware of the specific regulatory and contractual obligations. As an example, a specific amendment to BAA notification clause.

"I always let our CEO know when we suspect an issue and defer to her on Board communication. That being said, the Chair of our cybersecurity committee of the Board is always informed. The Cyber committee is always briefed at every quarterly committee. If an incident is confirmed, the Board is always briefed as is the committee. Same after the incident. Communication is critical."

Communicate Clearly During the Incident

During an active incident, the Board's needs are different from those of technical teams. Directors require timely, factual, and decision-oriented updates that focus on business impact rather than root-cause speculation. Effective CISOs communicate what is known, what is not yet known, and what is being done without certainty of inflation or minimization. Over-reassuring language early in an incident can damage credibility later.

Board updates during a crisis should be structured, consistent, and disciplined. At a minimum, communications should address five core questions:

1. What happened?
2. What is the current and potential business impact?
3. What actions are underway to contain and recover?
4. What decisions or support are needed from leadership or the Board?
5. When will the next update occur?

Legal counsel and crisis management experts may have specific requirements on what is included or excluded from communication.

"During an incident, I keep the Board focused on three things only: what we know, what we don't know, and what decisions may be required. Clarity and cadence matter more than detail."

CISOs should avoid overloading the Board with technical telemetry, timelines, or speculative attribution. Instead, communications should be synchronized with legal, risk, compliance, clinical, and operational leaders to ensure consistent messaging and to respect regulatory or law-enforcement constraints on disclosure. This coordinated approach reduces the risk of conflicting narratives and reinforces executive alignment during periods of intense scrutiny.

Manage Broader Stakeholder Communication

While the Board is a critical audience, it is not the only one. Employees, patients, partners, regulators, law enforcement, and third parties may all require communication during a cyber event. Effective CISOs understand that inconsistent or unauthorized messaging can amplify harm, fuel misinformation, and erode trust. Pre-established communication plans, templates, and workflows are essential to maintaining control over the narrative while allowing timely disclosure.

A comprehensive communication strategy, integrated with technical, operational, and clinical response activities, is particularly important in healthcare and other mission-critical sectors. Aligning communications across command

centers ensures shared situational awareness, protects safety and continuity, and reinforces the organization's credibility under pressure. For the Board, this coordination is a signal of maturity: it demonstrates that cyber incidents are being managed as enterprise events, not isolated IT failures.

Lead Post-Incident Communication and Continuously Improve

Crisis communication does not end when systems are restored. How CISOs engage the Board after an incident often has a lasting impact on trust and funding. Boards expect a structured, candid review that separates emotion from analysis and focuses on improvement rather than blame. Leading CISOs follow a formal framework to document lessons learned, control gaps, and prioritized remediation actions.

Post-incident communication should clearly articulate:

1. What worked as intended and should be reinforced
2. What did not work and why
3. What changes are being made to people, process, or technology
4. How improvements will be tracked and validated over time

Importantly, CISOs should close the loop by reporting progress against these commitments in subsequent Board updates. This reinforces accountability and demonstrates that incidents are being used to measurably strengthen organizational resilience.

Crisis Communication Key Takeaway for CISOs

Boards do not expect perfection during a crisis; they expect leadership, transparency, and control. How a CISO communicates before, during, and after an incident shows the Board how mature the organization's governance really is. Prepare the communication framework in advance, give updates that are clear and well timed, and close the loop on lessons learned. Doing so turns a high-pressure event into proof that cyber risk is being managed as an enterprise priority.

8. Conclusion: The CISO as a Strategic Partner

Effective Board engagement is never about a single presentation but a sustained discipline. CISOs who understand their Board, prepare thoroughly, align with fellow executives, and report consistently in business terms move cybersecurity from a technical concern to a recognized enterprise risk. By framing cyber risk around patient safety, operational resilience, regulatory exposure, and financial impact, and by pairing every risk with a clear plan of action, you give Directors what they need to fulfill their oversight responsibilities with confidence.

Trust built in routine meetings is what carries the organization through a crisis. By educating the Board over time, staying transparent about gaps and progress, and connecting security investments to the organization's mission, the CISO becomes a strategic partner in protecting patients, data, and the organization's future.

9. Appendix: Template for Phased Board Engagement

Phase 1: Foundational Engagement and Education (Meetings 1-2)

Objective: To establish a baseline understanding of cybersecurity as a strategic enterprise risk and to introduce the Board to the organization's current posture in business-relevant terms. This phase is about building trust and opening a channel for transparent communication.

“Before Your First Meeting" checklist: (1) request 1-2 years of prior Board/committee packs and minutes on cyber topics, (2) meet the committee chair 1:1 in advance, (3) confirm how the organization currently defines materiality and risk appetite, (4) review any open regulatory findings, audit findings, or prior commitments made to the Board before your arrival, so you can answer any prior representations.

Meeting 1: Cybersecurity as a Business Imperative

- **Frequency:** A dedicated session.
- **Key Topics:**
    1. **The "Why":** Start with the strategic context. Connect cybersecurity to the organization's core mission: patient safety, research integrity, and stakeholder trust. Use the "Board Interest" table from the primer to tailor your message. For a pharmaceutical manufacturer, for instance, frame the discussion around protecting high-value clinical trial data and intellectual property.
    2. **The Regulatory Landscape:** Provide a high-level overview of the legal and regulatory obligations specific to your sector, such as HIPAA, FDA guidance, and GDPR. Explain that compliance is the baseline, not the ceiling.
    3. **Introduction to NIST CSF:** Introduce the framework as the structure for all future cyber risk discussions, positioning cyber within the broader enterprise risk context.
    4. **The Six NACD Principles:** Briefly introduce the six principles as the "rules of the road" for the Board's oversight role. This frames their responsibility and your role in supporting them.

Meeting 2: Understanding Our Current State

- **Frequency:** A 60-minute session, ideally within the same quarter as the first meeting.
- **Key Topics:**
    1. **Threat-Informed Overview:** Present a high-level, threat-informed picture of the risks facing the healthcare and life sciences sector. Use examples like the NotPetya attack to illustrate systemic risk beyond a single organization.
    2. **Our "Crown Jewels":** Lead a discussion to review the organization's most critical data and systems ("crown jewels"). This is a crucial step in prioritizing protection efforts. For a health delivery organization, this would include patient records (PHI) and clinical systems.
    3. **Initial Gap Analysis:** Present a candid, high-level assessment of the current cybersecurity program against a chosen framework (e.g., NIST CSF). Crucially, report on the gaps rather than an "all green" status. Explain the business impact of these gaps and introduce the concept of a maturity roadmap to address them.
    4. **The "Three Lines Model":** Explain how cybersecurity responsibilities are structured within the organization using the Three Lines Model (Management, Risk/Compliance, Audit) to demonstrate

clear governance and accountability.

Phase 2: Build a Strategic Partnership; Define Risk Appetite (Meetings 3-4)

Objective: To transition from education to active partnership. This phase focuses on collaborative decision-making, quantifying risk, and formally defining the organization's tolerance for cyber risk.

Meeting 3: Defining Risk Appetite

- **Frequency:** A dedicated working session of 60-90 minutes.
- **Key Topics:**
    1. **What is the Risk Appetite?** Define risk appetite as the amount of quantifiable risk an organization is willing to accept in pursuit of strategic objectives. Use the analogy of financial literacy: not every Board member is an auditor, but all can read a financial statement. The goal is achieving similar “cyber literacy”.
    2. **Quantifying Risk in Business Terms:** Introduce **Key Control Indicators (KCIs)** as the primary method for reporting. Present a sample list of no more than 10-14 strategic KCIs, such as "% of critical assets recoverable in N hours" and "# of risk-accepted policy deviations".
    3. **The Risk Appetite Statement (RAS):** Facilitate a discussion with the Board to establish a qualitative RAS (e.g., Low, Medium, High) for cyber risk, comparing it to other enterprise risks and align it with the enterprise risk management processes. Explain that this will provide the "guardrails" for your program's priorities and investments.

Meeting 4: The Cybersecurity Strategic Plan & Budget

- **Frequency:** A 60-minute session, part of the annual strategic planning and budgeting cycle.
- **Key Topics:**
    1. **Alignment with Business Strategy:** Present a multi-year cybersecurity strategic plan that is explicitly linked to the organization's overall business goals. If the strategy includes launching new digital health services, show how the cybersecurity plan enables this securely.
    2. **Evidence-Based Budgeting:** Present the cybersecurity budget not as an IT cost center, but as an investment in risk mitigation. Justify spending requests based on their ability to improve specific KCIs and keep the organization within its stated risk appetite. Highlight what investments fell below the "cut line" and the associated risks the organization is accepting.
    3. **The Role of the CISO and Steering Committee:** Clarify your role and the role of an Information Security Steering Committee (SteerCo) composed of C-suite leaders (CRO, COO, CIO, etc.). This demonstrates that cyber risk decisions are made collaboratively across the business, not in a silo.

Phase 3: Ongoing Strategic Oversight and Reporting (Steady-State Cadence)

Objective: To maintain a continuous, strategic dialogue with the Board, provide them with the information they need to effectively govern cyber risk. This phase moves to a regular, predictable rhythm of communication.

Ongoing Board Communication Cadence:

- **Frequency: Quarterly reporting** to the relevant Board committee (e.g., Audit or Risk), with a summary report to the full Board at least annually. Ad-hoc updates should be provided for major incidents or significant changes in the threat landscape.
- **Standard Agenda Items:**
    1. **KCI Dashboard Review (The "Story"):** This should be the core of your report. Present a dashboard of the 10-14 strategic KCIs you established in Phase 2. Focus on **"telling the story**." Explain the trends, what they mean for the business, and how they compare to the agreed-upon risk appetite. For example, if the "Timely Patching" KCI shows a decline, explain the operational reasons and the potential impact on patient care systems.
    2. **Threat Landscape Update:** Provide a brief, curated update on the most relevant threats to the healthcare and life sciences sector. Focus on a summary of adversary tactics, techniques, and procedures (TTPs) that are relevant to your organization.
    3. **Incident and "Near Miss" Review:** Report on any major incidents and, just as importantly, significant "near misses". Near misses are valuable learning opportunities and demonstrate the effectiveness of your defenses.
    4. **Strategic Initiatives Update:** Briefly update the Board on progress against the cybersecurity strategic plan.
    5. **Regulatory and Legal Update:** Inform the Board of any new or changing cybersecurity regulations and their potential impact on the organization.

Continuous Engagement Outside the Boardroom (as permitted):

- **Build Relationships:** Establish one-on-one relationships with key Board members, particularly the chair of the committee with cyber oversight responsibility.
- **Share Information:** Provide the Board with relevant articles, reports, and threat intelligence between meetings to keep them informed.
- **Conduct Simulations:** Involve the Board in tabletop exercises and incident response simulations at least annually. This is critical for ensuring that they understand their role during a crisis.

10. Acknowledgments

The Cybersecurity Board Governance Task Group Leads – Inhel Rekik, Bracco Group; Janine Fadul, Universal Health Services; and Bill Reid, Google - wish to thank all the task group members who participated in this effort over the last 18 months, and in particular those who committed considerable time and thought in the consideration and drafting of this guide.

Nancy Brainerd, Medtronic

Joe Burgoyne, WS Audiology

Paul Connelly, formerly HCA Healthcare

Ty Greenhalgh, ServiceNow

Carter Groome, First Health Advisory

Judy Hatchett, Surescripts

Lenny Levy, RSM

William Retana, Medical Microinstruments

Kim Sassaman, Universal Health Services