CYE

Charting Success: **CISO's Guide to Cybersecurity Board Reporting**

Introduction

Despite Gartner's finding that 88% of boards of directors view cybersecurity as a business risk, communicating cybersecurity to the board from a CISO's perspective remains a challenge. Often, there is miscommunication when defining business objectives and cybersecurity priorities.

Bridging this communication barrier is essential for creating a comprehensive cybersecurity strategy that aligns with the organization's goals and business objectives.

This guide will explore the main challenges a CISO faces, address the common concerns of the board, how to effectively communicate cyber risks in quantifiable KPIs, and key components of board reporting to win approval and support for cybersecurity initiatives.

CISO Challenges

CISOs must overcome certain barriers when presenting their cybersecurity requirements to the executive C-level suite. Research taken from Harvard Business Review revealed that **"Just 69% of responding board members see eye-to-eye with their chief information security officers (CISOs)."** CISOs must find a way to create harmony and foster a more collaborative relationship with the board to effectively communicate the critical aspects of cybersecurity within the organization.

Addressing the following concerns is essential to preventing miscommunication.

- **The Language Barrier:** Translating complex technical jargon and presenting it in layman's terms is where miscommunication typically occurs. Conveying intricate cybersecurity metrics should be presented in a relatable language that the board can understand clearly. Data overload also presents confusion. It is important to keep the KPIs focused on the financial impact rather than on threat assessments. For instance, a CISO might explain that the financial implications associated with a potential breach far exceed the costs of remediation. The impact on business, including customer churn, litigation fees, regulatory fines, and loss of market share are all relatable terms that the executive board can process.

> **"A modern cybersecurity program must have board and executive level visibility, funding, and support. The modern cybersecurity program also includes reporting on multiple topics: understanding how threats impact revenues and the company brand."**
>
> Demitrios "Laz" Lazarikos, Founder and CEO, Blue Lava, Inc.

- **Lack of Quantifying Risk:** It simply isn't enough to showcase the critical assets of an organization that are the highest risk. Quantifying the effectiveness of preventative risk measures in terms of ROI justifies the investment. **Consider, for example, a security solution with an initial investment of $200K that substantially reduced organizational exposure by $2 million.** This specific example demonstrates a clear ROI and justification of cyber investments to the board. Demonstrating a clear ROI of cybersecurity investments can be challenging to quantify in financial terms if an organization doesn't understand which critical assets are at the highest risk. Focusing risk mitigation efforts without contextual business prioritization can lead to an inefficient allocation of resources, impacting an organization's ability to effectively protect its most valuable assets.

- **Justifying Budget:** Risk remediation efforts require having the right security tools to detect, prevent, and respond to cyber threats as they arise. CISOs cannot provide effective security measures if investments are limited or each decision requires persuading the entire C-level team to allocate funds. For example, an organization's legacy solutions are susceptible to known vulnerabilities, and upgrading existing legacy systems and infrastructure involves substantial investment. The CISO must justify immediate ROI to the board for approval and financial backing. A level of trust must be established for CISOs to perform their job as effectively as possible.

- **Compliance-Driven Focus:** The miscommunication barrier arises when there's an assumption that achieving compliance automatically ensures the organization's security posture. A compliance-centric approach may not adequately address evolving threats not explicitly covered by existing regulations. Furthermore, the board may struggle to notice the direct correlation between compliance metrics and the organization's strategic goals, potentially leading to a lack of support for any future cybersecurity initiatives.

"Just 69% of responding board members see eye-to-eye with their chief information security officers (CISOs)."

Harvard Business Review

Key Components of Board Reporting

Understand Your Audience

Board's Perspective on Cybersecurity: Boards evaluate the effectiveness of cybersecurity investments. Whether it's quantifying the tangible impact on business resilience, or ensuring alignment with strategic objectives, the board has an obligation to ensure that these investments yield returns in safeguarding the organization's assets and maintaining its overall security posture.

Let’s examine some common concerns from the board and how a CISO can proactively address them.

Board Concern	CISO Objective
Are we completely secure?	There is no way a CISO can guarantee that the organization is 100% secure, as there are many emerging threats constantly evolving in the wild. Demonstrating prioritized risk mitigation is an effective way to reassure the board as you are focusing your mitigation efforts on the risks with the highest returns for the business.
What additional investments are needed for new technological solutions?	Be transparent. This all depends on the current security posture of the organization. Performing a cybersecurity risk assessment can tell you if your existing infrastructure and technology stack is vulnerable. Although there might be newer cybersecurity solutions on the market that can provide great value in terms of vulnerability detection, risk mitigation, and ultimately breach prevention, it is vital to perform an ROI analysis for each new tool. Upgrading legacy systems and IT will no longer require justification to the board; it will become a validated necessity at this point.
Are our investments proving to be effective?	The board might be reluctant to allocate additional investments if there is no justifiable reason to do so. One way to justify the investment is to present the board with the true cost of a cyberattack as opposed to mitigation efforts. Cyber risk quantification (CRQ) establishes a clear financial context, enabling them to see the potential magnitude of losses without having effective security measures implemented.
Are we allocating our resources efficiently?	Ensuring business continuity is a top priority for any CISO. Benchmark your cybersecurity maturity and set measurable goals. Understand the potential financial impact of various incidents and build a mitigation plan as part of an effective cybersecurity strategy that is fully aligned with the organization’s business objectives.

Tailoring Reports to Board Members: Prioritizing risk mitigation is fundamental for overcoming board objections and other biases as it demonstrates a proactive approach to decision-making, aligning with the strategic business direction of the board. The board also has obligations to its shareholders to ensure long-term viability. Prioritizing risk mitigation reflects a commitment to fiduciary responsibility by preventing potential losses associated with unforeseen risks. A visual representation of the most critical business assets represented by risk severity can help garner the support of the board.

Strategic Alignment

Connecting Cybersecurity to Business Goals: CISOs must effectively connect cybersecurity to business goals. One way of achieving this is through competitive positioning in the market. A critical aspect of competitive positioning is how well an organization can handle cybersecurity incidents, reassuring the board that the organization is fully equipped to recover from major incidents. Having an actionable risk mitigation plan can further convince the board that you are making well-informed business decisions that extend far beyond traditional security measures.

Connecting Evidence-Based Value to the Organization: The primary obligation of a CISO is to ensure the overall security posture of the organization, first and foremost. For example, if an incident arises during non-business hours or in the middle of the night, the CISO must have an immediate incident response plan which includes identifying and remediating the threat as the organization's critical data assets may have already been significantly impacted. Each second counts and costs during the event of a breach. Case in point: Research taken from IBM's Data Breach Action Guide showed that it took **277 days on average to identify and contain a breach; 207 days to identify and 70 days to contain.**

Now factor in the time and resources it will take to mitigate the total damages. Ensure that the board comprehends the true financial implications and scope of a breach.

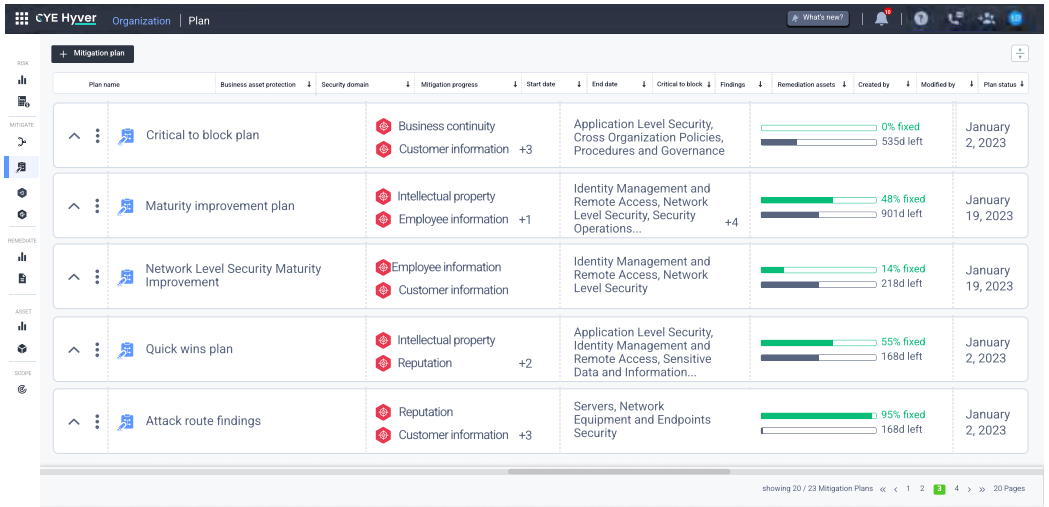
"Board and C-execs are pressured to strengthen the balance sheet and improve the profitability of the business. They have a number of challenges on their mind and cybersecurity happens to be just one of many."

Jitender Arora, Partner and Chief Information Security Officer (CISO) for Deloitte North and South Europe (NSE)

Communicating Cyber Risks and Business Impact

Clarity in Risk Assessment

Presenting Threats and Vulnerabilities: Not all threats are created equal. Chasing the low-priority ones might be costing your organization a substantial amount of resources and lost profits. By categorizing threats according to severity and probability, organizations can focus their efforts and financial investments on mitigating the most critical threats first. Effective cyber risk assessments begin by analyzing the organization's existing security plan, identifying vulnerabilities and their impact on critical assets, and mapping out attack routes before developing a mitigation plan.



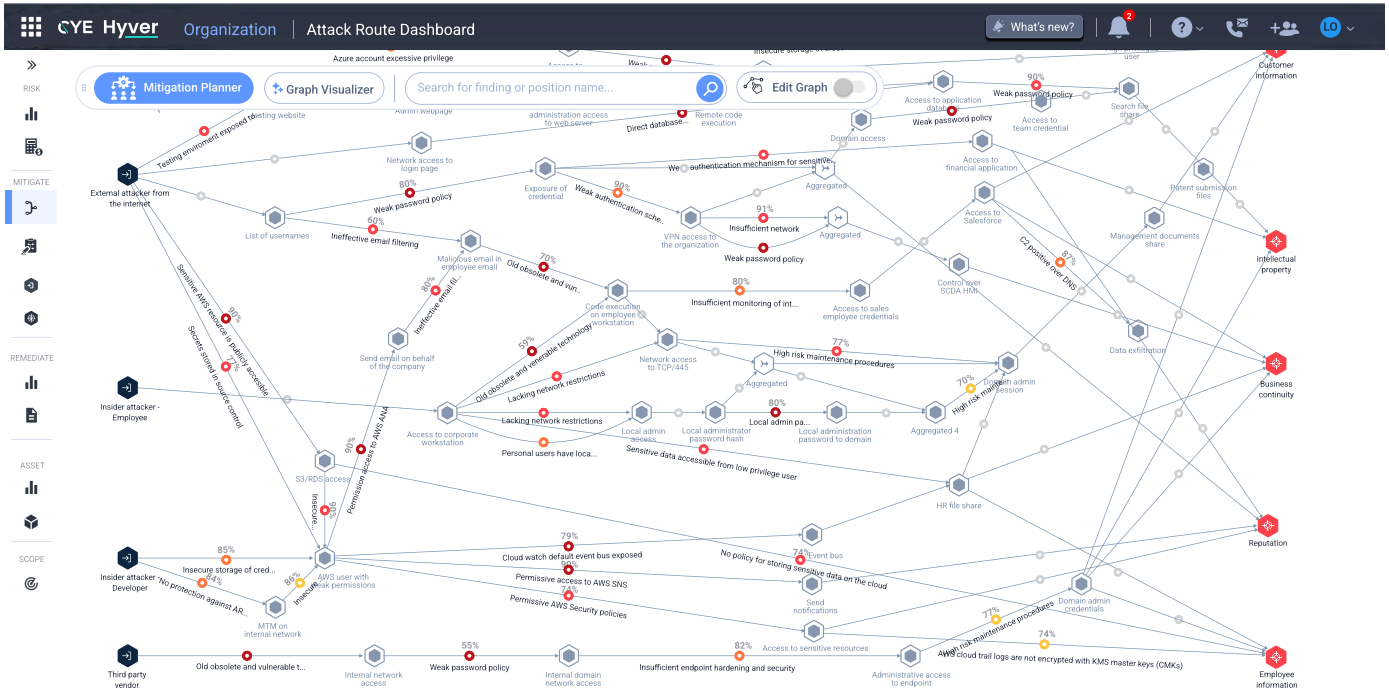
Assessing Potential Impact: Providing the board with real attack scenarios is essential for them to comprehend the feasibility of these actions. Cyber risk assessments help provide a framework for prioritizing threats based on their potential business impact. During a risk assessment, framing specific questions becomes instrumental in linking the CISO's business goals with the organization's long-term ROI.

Key questions to consider during a risk assessment:

- What is the potential financial impact of the identified risk?
- How might the risk impact day-to-day operations and business processes?
- How well-prepared are we to handle the consequences of this risk?
- How might this risk impact our profitability and financial returns in the long term?
- Can we hold third parties accountable in the event of a breach?
- Is there a clear understanding of which sensitive data assets are at most risk?

Addressing these questions not only enhances risk management but also contributes to the organization's overall cybersecurity resilience and sustained financial performance.

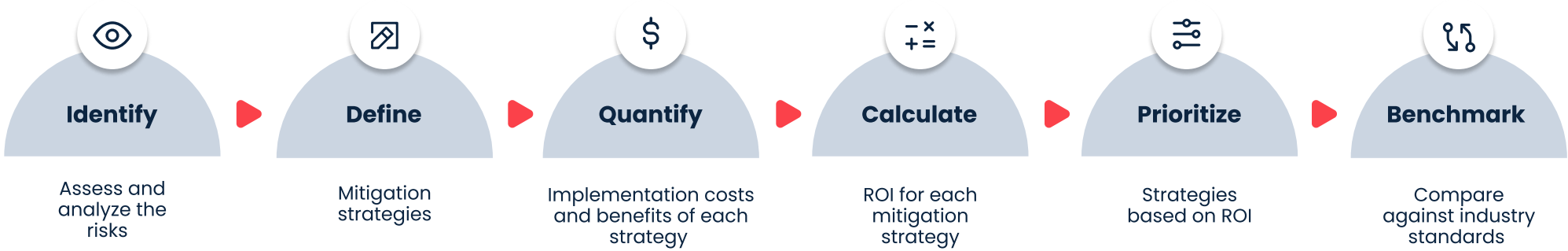
Mitigation Strategies



Proposed Solutions and Countermeasures: After a CISO has identified and prioritized business-related risks, the next step is to translate them into a concrete plan of action. Effective countermeasures such as continuous monitoring and threat intelligence, incident response plans, and attack route visualization must be implemented. Obtaining comprehensive visibility over your organization's probable attack routes through a detailed graph visualization helps make communicating cyber threats much clearer to the board and other key stakeholders.

Resource Allocation and Budgeting: Cyber investments are on pace to reach **$215B in 2024, a 14% YoY increase**. Conducting a cost-benefit analysis provides the board with a transparent understanding of the direction of resource allocation of cyber investments. This analysis enables a comprehensive evaluation of the anticipated costs associated with implementing specific mitigation measures against the expected benefits in terms of risk reduction, operational resilience, and long-term security enhancement.

A detailed example of a cost-benefit analysis for mitigation strategies



Armed with data-driven insights, CFOs can feel very confident allocating budgets for cybersecurity initiatives as they possess a comprehensive understanding of the risk landscape and the potential financial impact of cyber threats.

Enhancing Business Performance Through Board Reporting

Metrics and Key Performance Indicators: CISOs must define measurable KPIs that reflect the effectiveness of the security measures. The table below highlights the most effective performance indicators that will yield the attention of the board.

Key Business Performance Metrics	
Cost per Incident: Measures the average cost incurred per cybersecurity incident. This crucial KPI provides insights into the financial impact and the efficiency of incident response efforts.	**Cost of Reputation Damage Repair:** Expenses associated with repairing the organization's reputation after a cybersecurity incident. Factor in the potential loss of business opportunities, public relations, and expenses related to potential litigation fees arising from the incident.
Incident Closure Rate: Measures the percentage of security incidents that have been successfully investigated, resolved, and closed.	**Cybersecurity Insurance Premium-to-Loss Ratio:** The ratio of cybersecurity insurance premiums paid by the organization to the total amount claimed or paid out due to cybersecurity incidents within a specific period. A higher ratio may indicate that the organization is paying higher premiums relative to the losses incurred.
Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR): These metrics measure the efficiency of the cybersecurity team in detecting and responding to security incidents. These critical KPIs give you a baseline indication of whether your existing security systems and tools are effective enough.	**Mean Time to Contain (MTTC):** The average amount of time it takes for an organization to identify and contain a cybersecurity incident from the moment the incident occurs.
Percentage Reduction in Downtime Due to Security Incidents: Calculate the reduction in downtime resulting from security incidents, emphasizing the impact of cybersecurity measures on maintaining business continuity.	**Return on Security Investment (ROSI):** Ratio of financial gains or savings to the total cybersecurity investment. Quantifiable ROSI metrics include costs avoided with data breaches, reduced downtime, or protection against potential financial losses.
Percentage of Critical Vulnerabilities Remediated: The proportion of critical vulnerabilities that have been addressed within a defined timeframe. When assessing this KPI, it's essential to consider the impact of false positives as they can distort the accuracy of the remediation percentage.	**Regulatory Compliance Rate:** Ratio of instances where the organization is compliant with regulatory standards to the total number of regulatory requirements applicable to the organization.

Establishing Performance Benchmarks: Once the KPIs have been defined, the next step is to establish performance benchmarks. Identify relevant benchmarks within the industry and compare the organization's metrics to industry best practices for continuous improvement. By adopting this approach and comparing your organization's security posture against industry peers, you can gain valuable insights to effectively convey your proposed cyber risk objectives to the board.

How CISOs Can Win the Board Over

Actions and updates from the last board meeting

- Benchmark previous KPIs
- Propose investment recommendations based on prior risk assessments
- Detail prior incident response activities

Risk landscape updates

- Provide an overview of the current threat landscape
- Highlight critical vulnerabilities identified, their severity levels, and the potential risk exposure to the organization
- Analyze incident data and patterns collected

Important regulatory events

- Present any new industry updates
- Number of regulatory violations identified and resolved
- Changes in privacy laws affecting customer data handling

Cyber risk performance metrics

- Org risk status and trends
- Risk by business unit
- Risk exposure

ROI

- Quantify the ROI of any new tools purchased
- Cost savings achieved through security optimization measures
- Decrease in insurance premiums as a result of enhanced cybersecurity posture

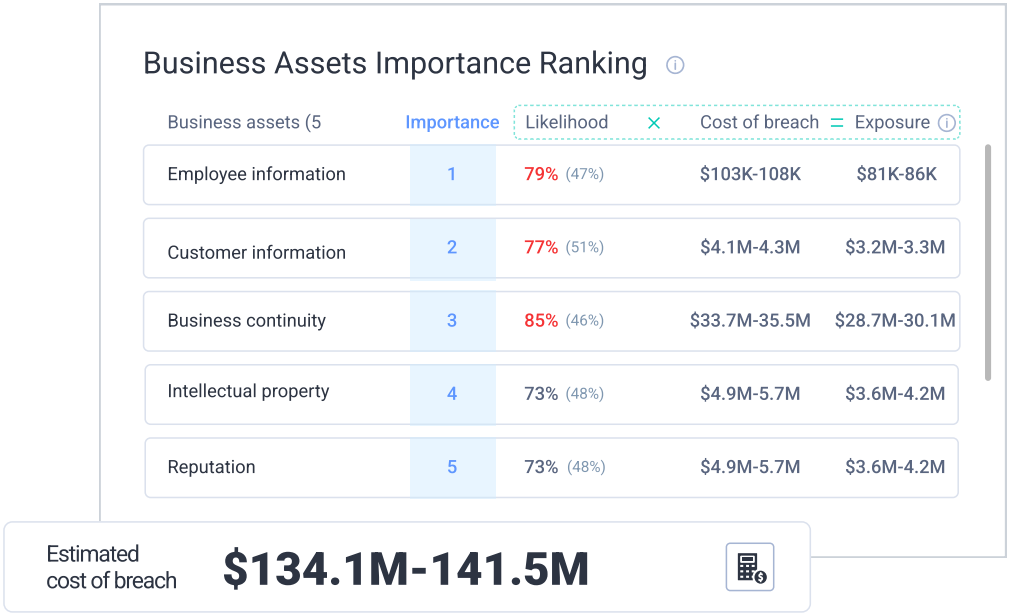
Executive summary

- Cybersecurity posture overview
- Threat landscape analysis
- Financial impact of security investments

The Empowering Impact of Hyver

Make communication with the board easier with CYE. Align your cybersecurity business goals with CYE's advanced cyber risk quantification (CRQ) platform.

- Hyver enables CISOs to create and execute optimized organizational security programs with significant business impact.
- Hyver's maturity model offers insights into potential cyber risks, allowing you to set targets, benchmark against your industry, and track progress over time.
- Hyver's ROI analysis tool enables you to effectively plan your cybersecurity budget and understand the financial impact of mitigation activities.



Gain complete visibility over your most critical business assets at the highest risk. Prioritize remediation strategies and make optimized mitigation decisions based on outcome. Maximize your ROI out of cybersecurity investments and gain crucial support from your board with CYE.

Want to learn more about CYE?
Contact us.

About CYE

CYE's optimized cyber risk quantification platform and expert guidance transform the way organizations manage cybersecurity. Using AI, machine learning, and extensive data, CYE visualizes attack routes, quantifies cyber risk, provides evidence-based mitigation plans, improves communication between CISOs and executives, and matures organizational cybersecurity posture. In doing so, CYE provides clear and relevant insights that empower companies to make effective cybersecurity decisions. The company serves organizations in multiple industries globally. Founded in 2012, with headquarters in Israel and operations around the world, CYE is funded by EQT and 83North. Visit us at cyesec.com.

CYE