The CISO’s Guide to Communicating Cybersecurity KPIs to the Board

We live in an increasingly interconnected, interdependent, and fragile digital world. If one domino falls, the whole line might topple over, as evidenced recently.

At the center of this fragile universe is the CISO, whose job isn’t just to keep fires from happening—and extinguish them quickly when they do—but to ensure they always have the resources they need to do their jobs well and protect company data from breaches, downtime, hacks, ransomware, and everything else.

That’s where communication with the board comes in.

CISOs play a critical role in bridging the gap between technical cybersecurity measures and business strategy. They’re responsible for ensuring that the board of directors understands the importance of cybersecurity and its impact on the organization’s overall risk profile. By effectively communicating the potential risks and the measures in place to mitigate them, CISOs help the board make informed decisions that align with the company’s strategic goals.

How can CISOs do this?

Key performance indicators (KPIs) are probably the most essential tool there is because they provide a clear, measurable way to track progress, highlight areas of concern, and demonstrate the value of cybersecurity investments.

Read on to learn how CISOs can best communicate cybersecurity KPIs to their boards and which cybersecurity KPIs to focus on.

Step 1: Understand the Board’s Priorities

CISOs often compete for resources with other departments. Understanding what the board values most helps CISOs make a compelling case for funding and support, ensuring that critical cybersecurity initiatives are adequately resourced. By understanding the board’s strategic priorities, CISOs can tailor cybersecurity initiatives to support these objectives, making security a business enabler rather than just a cost center.

Common board concerns include:

- **Risk management:** Boards are deeply concerned with identifying,

assessing, and mitigating risks that could jeopardize the organization's success. Cybersecurity is a significant aspect of risk management, as cyber threats can lead to data breaches, operational disruptions, and reputational damage. CISOs need to demonstrate how their security strategies mitigate these risks, protect key assets, and reduce the likelihood of business interruptions

- **Financial impact:** The board is responsible for overseeing the financial health of the organization. Cyber incidents can have a direct financial impact through losses, fines, and recovery costs, as well as an indirect impact through reputational damage and loss of customer trust. CISOs must illustrate how cybersecurity investments can prevent costly incidents and provide a return on investment by safeguarding the organization's financial stability.
- **Regulatory compliance:** Regulatory compliance is a top concern for boards because non-compliance can result in hefty fines, legal penalties, and damage to the organization's reputation. With the increasing complexity of global data protection regulations (like GDPR, HIPAA, etc.), boards expect CISOs to ensure that the organization meets all relevant compliance requirements. Failure to do so could have serious financial and legal consequences.

Once you fully understand your board's priorities, you're ready to dig into the KPIs—first, by choosing the best ones to focus on.

Step 2: Selecting Effective Cybersecurity KPIs

Selecting the right cybersecurity KPIs is critical to ensuring that cybersecurity efforts are aligned with the organization's goals and can be effectively communicated to the board.

Here are some criteria to consider:

- **Relevance:** KPIs should be directly related to the organization's cybersecurity objectives and broader business goals. For example, if protecting customer data is a top priority, a KPI focused on data breach incidents would be relevant.
- **Measurability:** Effective KPIs must be quantifiable. They should be based on data that can be consistently tracked over time, allowing for objective assessment.
- **Clarity:** KPIs should be easy to understand, especially for non-technical

stakeholders like board members. Avoid overly technical language and ensure that the metric clearly conveys its significance.

- **Actionability:** KPIs should provide insights that lead to actionable steps. If a KPI indicates poor performance, there should be a clear path to improving that area.
- **Timeliness:** KPIs should be reported at intervals that are appropriate for the decision-making process. Real-time or regular reporting ensures that stakeholders can respond quickly to emerging threats.
- **Benchmarking:** Choose KPIs that can be benchmarked against industry standards or past performance. This allows for comparison and helps in setting realistic targets.

Examples of Commonly Used Cybersecurity KPIs

Here are the most commonly used cybersecurity KPIs:

- **Mean time to detect (MTTD):** This KPI measures the average time taken to identify a security threat after it has occurred. A shorter MTTD indicates a more effective detection capability.
- **Mean time to respond (MTTR):** Also known as mean time to restore, MTTR tracks the average time taken to respond to and mitigate a security incident after it has been detected. This is crucial for minimizing the impact of breaches.
- **Number of detected incidents:** This KPI tracks the number of security incidents detected over a specific period. It helps in assessing the effectiveness of detection mechanisms and can be used to identify trends.
- **Incident response success rate:** This measures the percentage of security incidents that are successfully mitigated without significant impact. A high success rate indicates strong incident response capabilities.
- **Compliance rate:** This KPI tracks the organization's adherence to relevant regulatory requirements, such as GDPR, HIPAA, or PCI-DSS. Compliance is critical for avoiding legal penalties and maintaining trust with stakeholders.
- **Patch management efficiency:** This measures the percentage of systems that have been patched against known vulnerabilities within a given timeframe. Effective patch management reduces the risk of exploitation.
- **User awareness training participation:** This KPI tracks the percentage of employees who have completed cybersecurity training programs. A

higher participation rate suggests a more security-conscious workforce.
- **Cost per incident:** This KPI measures the financial impact of security incidents, including the cost of remediation, recovery, and any associated fines or legal fees. It helps in assessing the economic impact of cybersecurity efforts.

Step 3: Translating Technical Cybersecurity Terms into Business Language

One of the biggest challenges CISOs face is translating technical cybersecurity jargon into language that resonates with business leaders and board members. The technical nature of cybersecurity can make it difficult for non-technical stakeholders to grasp the significance of certain threats or understand the value of specific security measures. If not communicated effectively, this gap can lead to misunderstandings, underestimation of risks, or misalignment between cybersecurity efforts and business goals.

Key challenges include:

- **Complexity:** Cybersecurity concepts are often highly technical, involving details about threats, vulnerabilities, and systems that business leaders may not be familiar with.
- **Abstract nature:** Cybersecurity risks and solutions are sometimes abstract or intangible, making it hard to convey their urgency or impact in terms that resonate with the board.
- **Perceived disconnect:** Business leaders might see cybersecurity as a purely technical issue, disconnected from broader business objectives, which can make it harder to secure support for necessary investments.

Tips for Simplifying Complex Concepts without Losing Significance

To bridge the gap between technical jargon and business language, it’s essential to simplify complex cybersecurity concepts while preserving their significance. Here are some tips:

- **Use analogies:** Relate cybersecurity concepts to familiar business scenarios. For example, compare a firewall to a physical security gate that

controls who enters a building. This will help make it easier for board members to understand its function.

- **Focus on outcomes:** Instead of diving into technical details, emphasize the outcomes of cybersecurity efforts. For instance, rather than explaining the intricacies of encryption, highlight how it protects customer data and maintains trust.
- **Avoid technical terms:** Replace or minimize the use of technical terms and acronyms. Instead of saying “DDoS attack,” explain it as “a large-scale attempt to disrupt our online services by overwhelming them with traffic.”
- **Use visuals:** Diagrams, charts, and infographics can help simplify complex ideas. Visual representations of cybersecurity strategies, risks, and metrics can make the information more accessible.
- **Tell a story:** Frame cybersecurity issues in the context of real-world examples or scenarios that have affected other businesses. This approach makes the potential impact more relatable and easier to understand.
- **Highlight the business impact:** Whenever discussing technical aspects, tie them back to business implications, such as financial loss, legal consequences, or reputational damage.

Step 4: Anticipating and Preparing for Potential Questions from Board Members

Board members often ask questions that stem from their focus on risk management, financial impact, and regulatory compliance. Anticipating these questions can help you prepare thoughtful, informed responses that demonstrate your command of the subject and your alignment with business objectives.

Strategies to anticipate and prepare for potential questions include:

- **Knowing your audience:** Understand the individual background, concerns, and priorities of each board member. Are they more focused on financial risk, regulatory compliance, or reputational impact? Likely, some will care more about certain things while others will care about other things, but tailoring your preparation to their priorities can help you anticipate the types of questions they’re likely to ask.
- **Reviewing past discussions:** Look at minutes from previous board meetings or discussions to identify recurring concerns or questions. This can give you insight into what topics are most important to the board.
- **Preparing data and examples:** Be ready to support your answers with

data, real-world examples, and specific KPIs. For instance, if you expect a question about the cost of cybersecurity investments, prepare a breakdown of how these investments have prevented potential losses.
- **Conducting a mock Q&A:** Practice with your team or peers by conducting a mock Q&A session. This can help you refine your responses and identify any gaps in your preparation.
- **Preparing for the "what if" questions:** Board members often ask hypothetical questions to understand potential risks and responses. Prepare scenarios that address "what if" situations, such as, "What if we experience a major data breach despite our current defenses?"

Handling Difficult Questions and Steering Discussions Back to Key Points

Difficult questions can arise, especially if board members are concerned about risks or uncertain about the value of specific cybersecurity initiatives. It's important to address these questions confidently and steer the discussion back to the key points you want to emphasize.

Strategies for handling difficult questions include:

- **Staying calm and composed:** Maintain a calm demeanor, even when faced with challenging questions. This helps to project confidence and control over the situation.
- **Acknowledging valid concerns:** If a board member raises a valid concern, acknowledge it. For example, if they express worry about the cost of a cybersecurity initiative, you might say, "That's a great point, and cost management is a key consideration in our strategy."
- **Providing clear, concise answers:** When answering difficult questions, be clear and to the point. Avoid overly technical jargon and focus on the business impact. For example, if asked why a particular security measure is necessary, explain its role in protecting the company's most valuable assets.
- **Using data to support your answers:** Whenever possible, back up your responses with data or specific examples. For instance, if questioned about the effectiveness of a security measure, reference the relevant KPIs that show its impact.
- **Redirecting to key points:** If a discussion veers off-topic or becomes too granular, gently steer it back to the key points. For example, "While that's

an important detail, what I'd really like to emphasize is how this initiative aligns with our broader goal of reducing risk and ensuring compliance."

- **Offering to follow up:** If you don't have an immediate answer, it's okay to acknowledge that and offer to follow up. "That's an important question, and I want to make sure I provide you with the most accurate information. I'll get back to you with more details after the meeting."

Remember: Honesty goes a long way in building good relations with the board. Board discussions can be difficult, but you'll make them much more difficult than they need to be if you're not transparent. Attempting to gloss over challenges or present an overly optimistic view can backfire if issues arise later. Being upfront about risks, limitations, and uncertainties also builds trust and demonstrates integrity.

Conclusion

If there's one thing a CISO needs to do really well, it's communicating cybersecurity KPIs to the board. By understanding board priorities, selecting the right KPIs, effectively communicating these KPIs by translating technical jargon into "board speak" via things like visualization and storytelling, and preparing for the hard questions, the CISO can succeed in gaining board trust on all things cybersecurity. Remember that communication is key, and never stop refining your approaches. Above all, commit to always being transparent so that you can build trust.

Learn more about how using Pure Storage enhances risk mitigation, ensures safe and secure data, and enables always-on protection.