XM Cyber

Guide

A CISO's Guide to Reporting Cyber Risk to the Board

Just How Elevated Have the Cybersecurity Stakes Become for Today's Organizations?

You've probably been there before – it's been a long day of putting out fires while trying (wherever you can fit it in) to develop long-term strategies to reduce risk and improve organizational security posture.

As you're packing your bag to head out, you notice an invite pop up in your email:

"Board <> CISO, Status Check"

Your pulse quickens, your pupils dilate more than you care to admit, your throat goes dry.

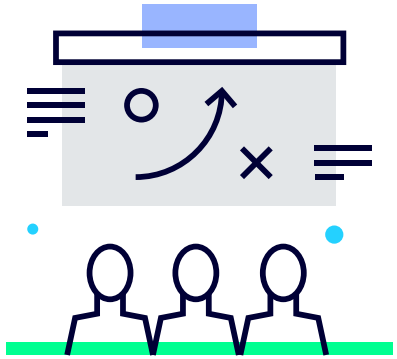
You've just been tasked with reporting your organizational security risk posture to the Board.

Now that cybersecurity has become a top concern for Boards and Execs alike, it may seem like everyone's got questions that you need to answer: Are we protected from threats? How have we improved or gotten worse over time? Can XYZ (feel free to insert name of any CVE that keeps you up at night) impact us?

Moreover, they want answers in terms that can be easily understood and correlated back to business-drivers and bottom lines – not lengthy technical discourse on remediation priorities and processes. Essentially, what ends up occurring is a disconnect between your position (CISO) and the Board to whom you report – a failure of communication that leads to misunderstanding, unnecessary risk, and "worst-case scenario" cyberattack outcomes.

So how can you report risk to your board in terms that can be quantified and understood by all for optimized outcomes?

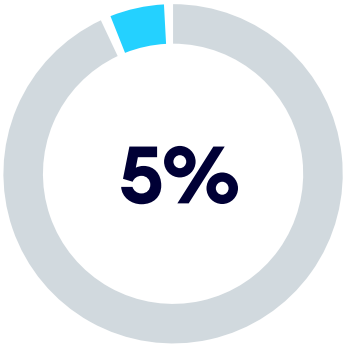
In this ebook, we will explore the factors that lead to challenges in communication and explore ways to finally report to the Board confidently and accurately.



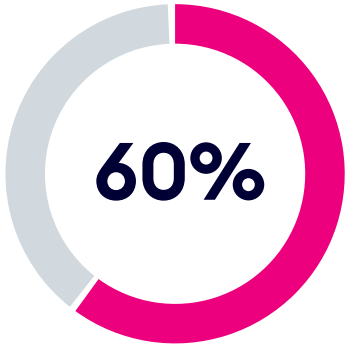
XM Cyber

Reporting Cyber Risk: Even When it's Done, it's Rarely Done Right

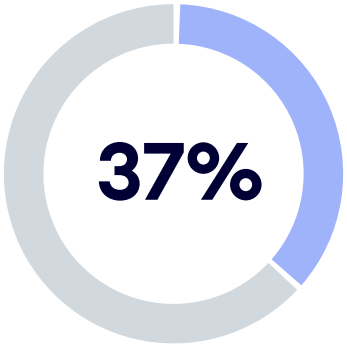
As CISO, you deeply understand the cybersecurity risks facing your organization. But there are often structural problems that prevent your all-important insights from making their way to the key decision-makers who need them.



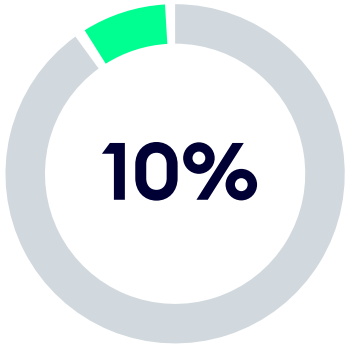
According to Heidrick and Struggles, leading executive consulting services, only 5% of CISOs report directly to the CEO, indicating a potential lack of high-level influence, **and 2/3's of CISOs are two levels down from the CEO in the reporting structure.**



Even worse: Among that 60%, nearly half report such briefings occur exclusively in the wake of a newly discovered security problem.

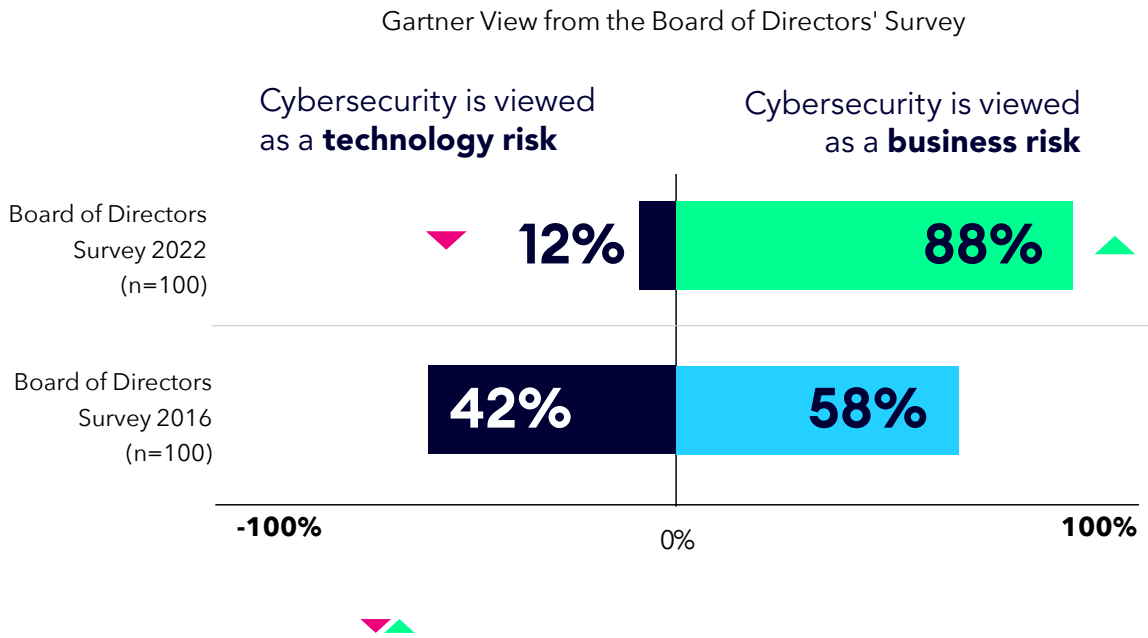


The majority of cybersecurity leaders report being at least three steps away from the CEO in the reporting structure, while **only 37% report that their organization effectively leverages their expertise.**



According to Gartner, ONLY 10% of boards have a dedicated cybersecurity committee overseen by a board member, though that number is expected to quadruple in just 5 years.

Encouragingly, however, the percentage of **board-level leaders who view cybersecurity as a direct business risk rose from 58% to 88% over a six year period.**



These numbers make it clear that serious shortcomings exist within corporate reporting structures and Board reporting procedures. Yet even as your involvement as a CISO becomes more direct, the problem of effectively communicating risk to the business remains.

The Challenges of Reporting

When reporting risk as a CISO, you must wrestle with the question of explaining technical problems to a largely non-technical audience.

When one is extremely well-versed in a subject, it's not always easy to know where to begin when conveying information to people with less grounding. The "curse of knowledge" often rears its head in Board reporting scenarios, so it's important to make sure that problems, solutions, value propositions, etc. are all clearly and concisely articulated in business language that resonates with them.

It also helps to have clear and quantifiable metrics to lean on. These metrics will ultimately impact key decisions on budget, resources, and affect the overall security posture of the organization.

Historically, IT was once perceived as a massive cost-center with limited impact on the bottom line. Cybersecurity still sometimes falls under that shadow today.

Shifting the perception of cybersecurity from cost-center to business-enabler should be a key priority for CISOs. That's not always easy to do without a simple and intuitive demonstration of ROI on security investments. Part of this includes quantifying risk in a way that truly reflects what is at stake.

4 Key Challenges Organizations Face When Reporting Risk to the Board

1

The ability to quantify the risk of breach to business-critical assets across on-premises and cloud environments through a single pane of glass.

2

Identifying the risk of potential M&As and the steps necessary to mitigate them.

3

The path of least cost for maximum impact on the organization's security posture and where to focus remediation efforts to get there.

4

The impact of security investments to security posture over time.

How Current CISO Reporting Fails to Meet These Challenges

A common, flawed approach to reporting is the recitation of conventional figures (how many vulnerabilities, incidents, patches etc. and how those numbers change over time) without applying real insight. This approach is a rough yardstick of progress. Lengthy discourses about security team actions, based on conventional metrics, can create white noise and obfuscate the real heart of the matter:

Are your most important assets safe?

Likelihood of Threat is an Area Where Wires Often Get Crossed

Likelihood can be calculated in multiple ways.

First, we can examine statistical data. It's possible to extract insights from analysis of past statistical data, but this omits the context of a specific organization – the specific threat landscape, changes in the environment, the full range of exposures they need to address, the assets that are most business-critical for the particular organization, etc. Ultimately, as a CISO, you need to convey this full and context-based picture of risk. Without a refined understanding of all of these elements, it's impossible to answer questions such as "Are we secure?" or "Are we improving?"

And without real answers to those questions, risk reporting becomes an exercise in futility.

The Risk Equation

RISK = LIKELIHOOD X IMPACT

Risk can be simply explained as the intersection of likelihood and impact: How likely is a successful cyberattack and what would be the cost to the organization if this occurs?

There Has to be a Better Way to Report Risk

To understand whether an organization's most critical assets are safe, it's imperative to have visibility into how things change over time, and how those changes affect risk.

Modeling to predict the likelihood of an attack is one way to do this. This approach provides a consistent predictive model that cuts through the noise of what can be bypassed, and what cannot, and contextualizes this information within the framework of critical assets.

Boards need to understand the likelihood of compromise and the impact that could occur to business-critical assets. These risks should be contextualized to each part of the business. For example, risks to ERP services, business services, cloud environments, customer databases, etc.

Boards need visibility into business insights and real-world ramifications. They need to understand the efforts being made to reduce risk and how these efforts are paying off.

In the face of an incident, will your stakeholders stand up in front of the cameras and defend their cybersecurity investments?

As CISO, you must explain the business value of any security investment you make and have metrics that define specific, agreed-upon protection levels.

More importantly, when reporting risk, it is not about security tools but the actual metrics that drive business decisions. Nonetheless, a CISO must be able to defend their security program with their key stakeholders. If your reporting delivers on outcomes and not a laundry list of issues, you can realize your organization's goals.

Most importantly, they need answers to the key questions:

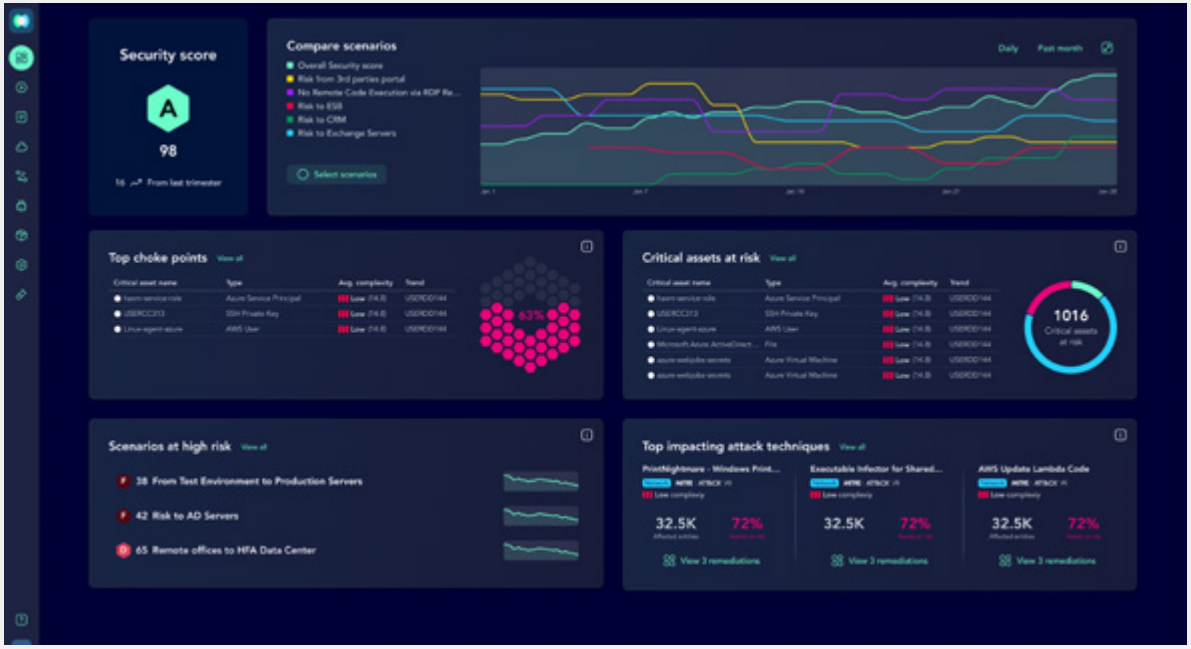
- What can be compromised today?
- What is the likelihood of that happening?
- What is the aggregate impact?
- What is the level of operational risk?

The Optimal Way to Report Risk to the Board

For reporting to achieve the desired effect, a new approach is needed. This approach should leverage the ongoing and holistic methodology of the Continuous Threat Exposure Management (CTEM) framework by Gartner®. CTEM continually assesses the entire ecosystem, including networks, systems, assets, and more, to identify exposures and weaknesses to reduce likelihood of impact.

With the XM Cyber Exposure Management Platform, organizations can benefit from a CTEM-based approach to reduce risk and improve posture. The platform provides valuable prioritization and guided remediation, as well exec-level reporting and posture trending to clearly communicate status and posture. Now CISOs and their team can demonstrate how attackers compromise critical assets across hybrid environments. It grants clear, context-based insights into all exposures, with sophisticated attack modeling to map all possible attack paths an attacker could take due to misconfigurations, vulnerabilities, overly permissive identities, etc. to compromise business-critical assets. It also quantifies risk to critical assets and shows which techniques can be used to get to them, focusing remediation efforts.

With the graphical visualization of the attack surface, you can see how a combination of exploits chain together to form attack paths from breach points to critical assets. The platform dashboard enables you to monitor your environment's security posture at a glance and provides actionable intelligence so you can tackle your scenarios, secure your critical assets, fix choke points, and remediate the most impactful exposures.



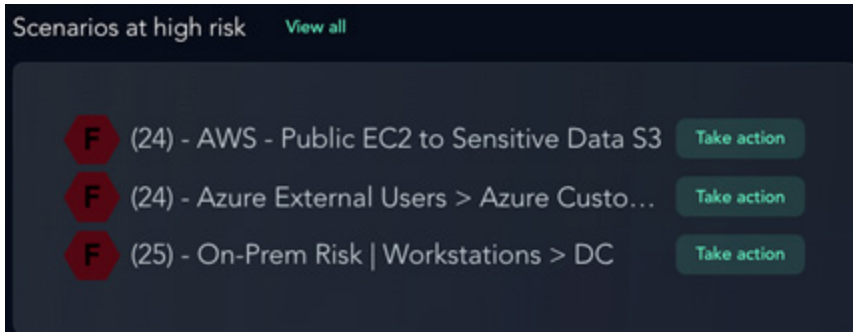
Unified view to track all critical assets providing continuous cyber security posture management via the XM Cyber Exposure Management Platform

Security Score

The security score widget shows the average security score of all the scenarios running in your environment. Once attack scenarios have been sufficiently modeled, XM Cyber scores the level of risk to the organization. The score of a scenario is based on how easy it would be for the attacker to compromise the critical assets. As you remediate security exposures, the security score improves, indicating better IT hygiene.

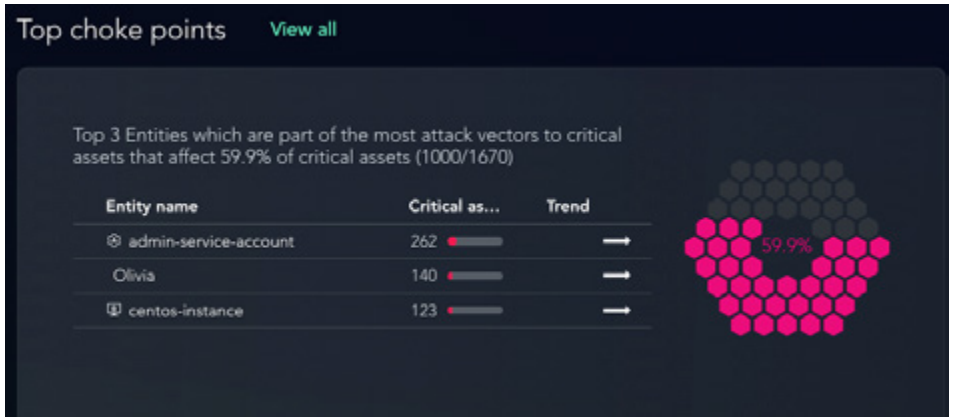
Compare Scenarios

Below the score, you can see whether you're trending up or down in the time range selected. When you use the Compare Scenarios trend graph you gain immediate insights into Scenarios at Risk, Top Choke Points, Critical Assets at Risk, and Prioritized Remediations, all of which we will delve further into below.



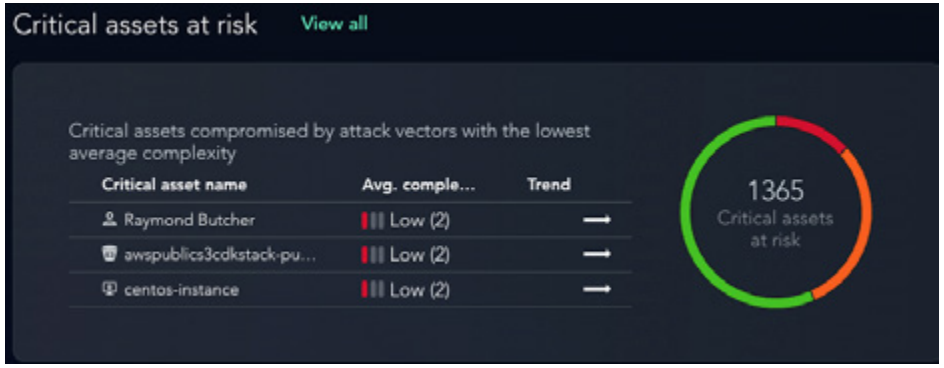
Scenarios At High Risk

XM Cyber enables you to prioritize which scenarios to improve first. When you view all the scenarios at high risk, you view the scenarios with the lowest scores and improve these scenarios first. You can even view a specific scenario and its trend by drilling down or you can "take action" to tackle this scenario and follow prioritized guided remediation steps.



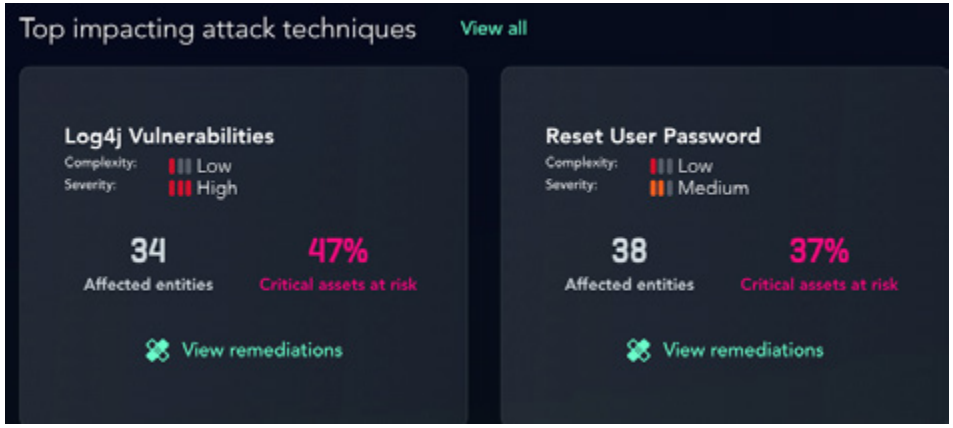
Top Choke Points

The table shows the three entities that attack paths most frequently cross on their way to your critical assets. These are the choke points in your environment. They put your critical assets at the most risk. The graph shows you the percentage of critical assets that the top three choke points lead to. Fix these top three choke points first. It won't necessarily harden all your critical assets, but it will give you high ROI of least cost and maximum impact to your security posture. Drill down into the choke point to disrupt the most damaging attack paths and follow prioritized guided remediation steps.



Critical Assets At Risk

You can also prioritize which critical assets to secure. The table shows the critical assets that are at risk and the attack paths with the lowest complexity. Paths with low complexity are easier for the attacker to compromise. The ring graph breaks down your critical assets by the complexity of the attack paths leading to them. A sizable percentage of your critical assets are on attack paths with low complexity, so harden these critical assets first.



Prioritized Remediation

Prioritized remediation helps ensure that security teams fix the most pressing issues, while security scores update in real time to show the likelihood of compromise. Risk can be broken down by specific scenarios. For example, XM Cyber can show whether an attacker can move from marketing endpoints to a customer database.

Attack modeling scenarios aligned with business goals to focus security posture hardening

With the XM Cyber Exposure Management Platform, you can confidently report risk to your Board accurately and comprehensively and demonstrate:

- How their organization can be attacked.
- How improvements are occurring over time because of security investment, change in processes or implementation of environment hardening.
- How much risk exists for critical assets.

XM Cyber

Six Key Security Questions XM Cyber Answers

1
What percentage of my critical assets are at risk at any given time?

2
What are the risks?

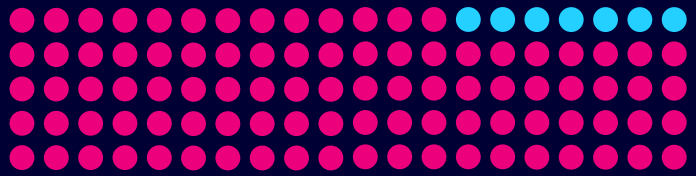
3
What do we need to remediate first to significantly impact our risk level?

4
Are our investments paying off? Are my protection levels increasing?

5
Do we have sufficient resources to handle the risks?

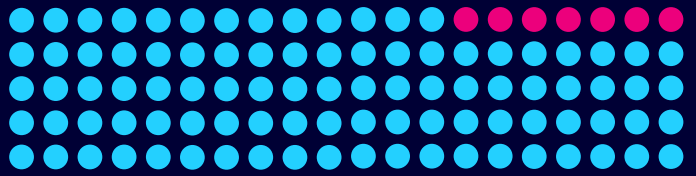
6
How are we improving over time?

Prioritized remediation reduces attack surface and hardens security posture



93% of assets have been compromised by the virtual hacker

Three months later



7% Only 7% of assets have been compromised by the virtual hacker!

Remediating the CISO<>Board Reporting Gap

CISOs have historically struggled to connect with Boards and convey a clear picture of risk in relation to the business and what return on investment their security stack is delivering. But with a CTEM-based approach, delivered with the right toolset, Board members will walk away from meetings with a much more powerful and quantifiable understanding of the most important questions they need answers to.

XM Cyber

XM Cyber is a leading Continuous Exposure Management company that transforms the way organizations approach cyber risk, enabling security teams to prevent more attacks with 75% less remediation effort. Its XM Attack Graph Analysis™ capability discovers CVEs, misconfigurations, and identity issues across on-premise and all major cloud environments. It analyzes how attackers can chain exposures together to reach critical assets, identifies key "choke points", and provides remediation guidance. Founded by top executives from the Israeli cyber intelligence community, XM Cyber has offices in North America, Europe, APAC-Japan, and Israel.