Cymulate

Four Cybersecurity Essentials for the Board of Directors

2022 Edition

Table of Contents

Explaining your organization's security strategy and controls to a non-technical audience can be challenging. Aligning that strategy against ever-changing threats and cyberattack techniques is even harder. Translating the strategy, threat landscape, and daily impact into meaningful risk metrics has traditionally been nearly impossible. Yet, executive teams and boards of directors are asking for precisely that. They increasingly demand data that describes the potential impact of a security threat to operations, brand reputation, market position—even stock value. This document provides a context for understanding the information a board needs and why. It will give you four insights based on quantifiable metrics to help you explain your current cybersecurity posture, defensibility, priorities, and funds allocation effectiveness in a language understandable and convincing to the board.

01 | Communication Closing the Gap

Every executive team—regardless of company size—cares about business risk. No one wants to make headlines for being the victim of a data breach. No longer "just an IT problem" or a minimum compliance requirement, cyberattacks are today a significant business risk. Leaders actively trying to manage risk have realized that cyber threats now represent the lion's share of potential harm, and they want timely risk metrics aligned with business priorities. ESG (Enterprise Strategy Group) 2021 “The Life and Time of Cybersecurity Professionals” survey shows that, among cybersecurity professionals’ top priorities:

- **41%** want cybersecurity participation in all business planning and strategy
- **38%** want to improve the ability to identify and quantify cyber-risks as they apply to the business

As executives’ priorities typically include ensuring that business imperatives are not hampered by security requirements and working with quantified evaluations, these trends amongst cybersecurity professionals should be encouraged and nurtured by executives.

Communication between business leadership and tech staff

Measurements of cybersecurity program effectiveness

Readiness for latest threats and compliance requirements

Spending optimization and rationalization

Figure 1: Cyber security concerns of boards and executive leadership

This convergence of view can also be leveraged to ensure continued compliance regardless of the upcoming compliance updates foreshadowed by governmental activity related to cybersecurity recommendations.

As ransomware and supply-chain attacks plague the networks, governments enter the fray. Between May and August 2021, USA Biden Administration issued an Executive Order to Improve the Nation's Cybersecurity, sent a memo with practical cybersecurity recommendations, took additional actions to protect critical infrastructures, passed the K-12 Cybersecurity Act into Law, and generally took numerous steps to raise awareness and impose additional cyber-security measures and recommendations.
In Europe, the Cybersecurity Act strengthens the EU Agency for cybersecurity (ENISA) and establishes a cybersecurity certification framework for products and services.
These herald an era of upcoming cybersecurity legislation across all sectors.
In addition, the Harvard Business Review reported that the SEC has begun to consider cyber vulnerabilities as an existential risk for businesses. For the CISOs, IT, and security professionals who must prepare and deliver reports to the board, the tightening of cyber-security regulations requires improving their security resilience and acquiring capabilities to monitor, measure, and track both resilience and security drift.

Aside from compliance considerations, the unabated rise of cyber-threats number, complexity, and scope turned cyber-risks into business risks and compelled executives to evaluate their potential impact on operations and revenues, not to mention the legal implications. Executives now have to communicate with their security team to establish what is essential or genuinely material to the company's operations, finances, and reputation. This requires presenting all the relevant data in a report understandable by non-tech people.

For cyber-security operatives tasked with preparing such reports, it helps to remember that the executive team and board members care about the cost of defending against cybersecurity vulnerabilities and attacks—not the technical details. They want Key Performance Indicators (KPIs) and metrics, not reports detailing software patches across thousands of systems. The following four paradigms can guide you in preparing an effective presentation.

Your Current Security Posture

Risk is always present. You need to identify and quantify which risks really matter to the company. Aligning your cybersecurity risks with the overall business strategy and critical assets is a good start. The first step to assessing and hardening the security posture is to answer a few questions:

01 What business goals are critical to the company's ability to survive and thrive?

02 Which processes and functions support those goals?

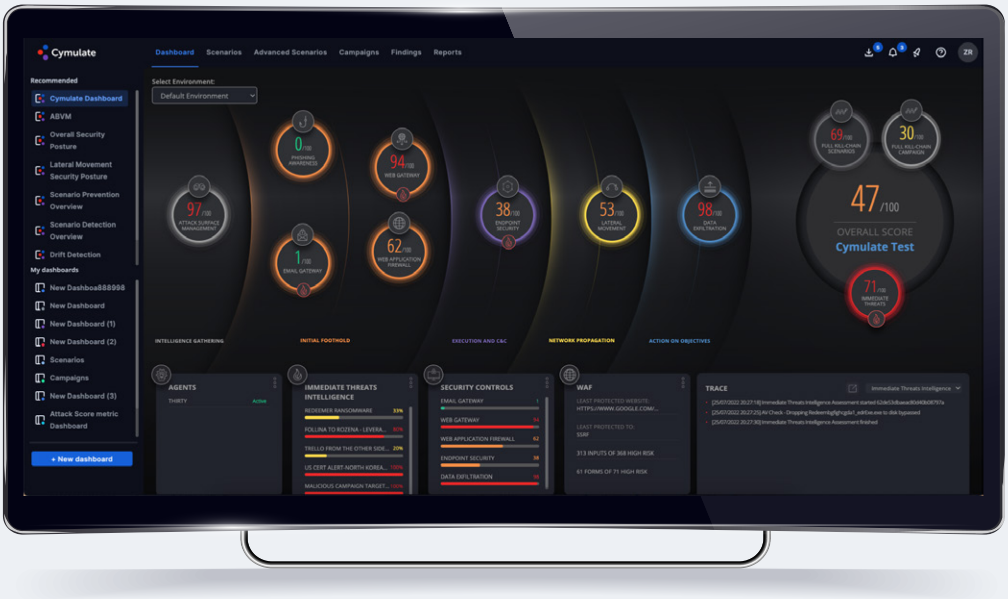
03 What are customer data's most critical assets to support these processes? Intellectual property? Proprietary processes? Specialty or customized equipment? Consumer-facing applications?

04 Where do these assets reside in the organization?

05 Which IT systems, applications, policies, or other technologies store, transmit, and use data and/or execute actions based on these assets?

Identifying what is critical and needs maximum protection makes detecting and evaluating coverage gaps easier. Reviewing external and internal controls provides current data on the active cyber-defense infrastructure. Measuring its actual effectiveness provides accurate information for a real-time security posture quantified evaluation, yielding a precisely measured exposure score. The most effective way to obtain quantifiable benchmarks for an immediate, objective understanding of vulnerabilities and risk levels is by testing security controls and challenging their effectiveness with simulations of cyber-attacks.
Attack simulations do exactly that. They challenge your existing controls' effectiveness across vectors so you can test them from an attacker's perspective and assess how well they would perform under a genuine cyber-attack.

Figure 2 below provides an example of benchmark data that enables you to assess the organization's security posture quickly and easily. The numeric and color-coded scoring gives an immediate understanding of your security posture health. A score of 100 means a shy-high probability of compromise. The lower the score, the lower the risk of compromise. The numbers' colors ranging from green (no worries), yellow (slight concern), orange (requires attention), and red (demands action), immediately show which part of your infrastructure is more at risk. Attack simulation results provide the foundation for knowing where you stand today. According to EY analyst Stephen Klemach, understanding escalation protocols, assessing the efficiency of the risk management program, defining risk tolerance, and monitoring security drift are all becoming an integral part of board practices.



```
[25/07/2022 20:27:18] Immediate Threats Intelligence Assessment started 62de53dbaead80d40b08797a
[25/07/2022 20:27:25] AV Check - Dropping Redeembgfighcgda1_edrExe.exe to disk bypassed
[25/07/2022 20:27:30] Immediate Threats Intelligence Assessment finished
```

Figure 1: CBenchmark data to assess active security posture end to end

Implementing an Extended Security Posture Management approach:

- Enables a common understanding of the cyber risk ecosystem through quantified benchmarks, baselining, and trending
- Consolidates and automates risk assessment and evaluation, decreasing overall effort and training needs
- Realizes cost savings by removing duplication, optimizing existing technologies decommissioning unnecessary legacy systems

02 | Measurements: Precisely Evaluate Risk Based on Documented Events

Historically, cyber risk has been evaluated through a combination of guestimates detection and response solutions' efficacy, based on the number of attacks and vulnerabilities detected fine-tuned by infrequent periodic guesstimates correction through penetration testing exercises.

The acceleration of the threat landscape expansion and the fluid nature of infrastructure in the day of IaaS and agile development are rendering these risk evaluation methods increasingly unreliable and unable to provide the resiliency that underlines compliance regulation updates (i.e., March 2022 PCI DSS v4.0 publication.)

To effectively assess your security posture, it Is imperative to test its ability to withstand attacks, which can only be truly measured by running a comprehensive array of attack emulations and measuring the delta between the number of attack emulations launched and the number of attacks detected, mitigated and/or stopped.
Cymulate's XSPM translates this delta into a security score associated with the color-coded risk level displayed in the dashboards (see above) and in the automatically generated downloadable executive and technical reports.

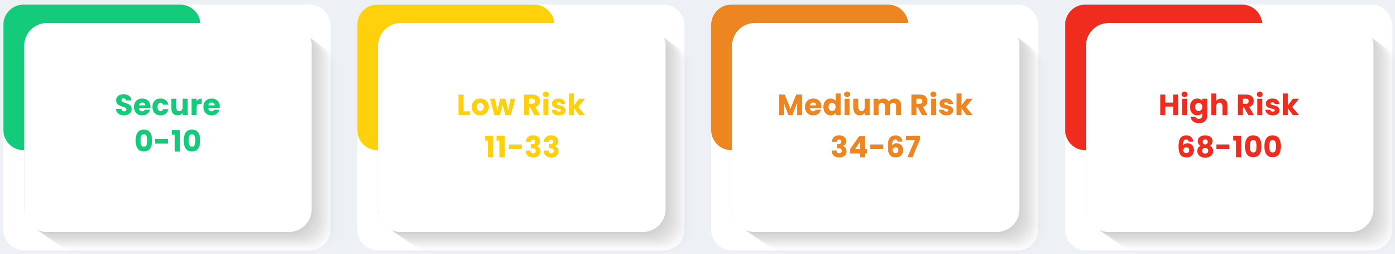


Figure 3: Cymulate Security Scoring Legend -scores and color-code

Assessment Frequency and Depth Matters

With new threats detected daily, the more frequently and continuously your security team runs assessments to test your infrastructure resiliency, the faster you will be able to ramp up your defenses. With attackers changing tactics depending on their goals and continually evolving techniques to increase their capabilities, your cyber team needs to

Easily access an attack emulation library that is always up to date
Example 1: when the Log4j Apache server vulnerability took the world by storm in mid-December 2021, you could have checked if your environment was affected or vulnerable or if the successive patches applied were effective.
As exploits such as Log4Shell immediately took advantage of the opportunity to execute code from LDAP servers, Apache servers' users around the globe scrambled to patch the supply-chain-induced vulnerability.
Example 2: two critical Microsoft vulnerabilities, CVE-2021-42287 & CVE-2021-42278, AKA Invoke-noPac, potentially paving the way to privilege escalation and relatively trivial to exploit, also endangered user’s cyber-resilience.

Automating immediate threat detection through an appropriate, regularly updated, Immediate Threat Intelligence module integrated into your security framework optimizes your controls faster and easily conveys the organization's resiliency to the newest attacks in the wild.
When asking your cyber team if your infrastructure is safe against the latest attack hitting the headlines, a well-equipped cyber team will be able to answer with certainty and /or give you a quantified evaluation of the risk factor and, if applicable, the time and resources needed to achieve optimal protection against that threat.

Have the ability to automate intelligent attack emulation that covers the entire kill chain to mimic attackers’ ability to run attacks that intelligently redraft the initial attack route when blocked and attempt to find an alternate route.

03 Readiness: The Business Side of Cyber Risk Evaluation

To collaborate efficiently with your cyber team in quantifying the various aspects of cybersecurity risk quantification, it helps to keep in mind a few elements that the cybersecurity team will need to integrate in their prioritization process to work in tandem with the board objectives.

What Is at Risk?

Prioritizing remediation efforts requires knowing which assets are most at risk and their relative levels of importance. This relates to the SEC's interest in material risks.
Which compromised assets and processes would result in serious operational, financial, or reputation damage to the company? Using overall business goals as a guideline, are external assets more critical than internal resources? If your customer-facing web portal is breached, would that be more important than if DevOps systems testing your next generation of software were compromised?

How Likely Are Specific Threats?

Another aspect of determining material risk is the likelihood of specific threats occurring. Who would want to attack your company's assets and why? Keeping up with cybercrime trends can help answer this question. Malicious attacks caused by hackers or criminal insiders continue to be the leading cause of data breaches, costing an average of US$ 4.62 million per breach, according to the IBM/Ponemon Cost of a Data Breach Report 2021. The pace of cyber-attacks continues to accelerate, with the average number of attacks per company rising from 206 per year in 2020 to 270 per year in 2021, according to Accenture State of Cybersecurity Report 2021. Increasingly core systems and industrial controls are attacked with the goal of disruption or destruction.

What Is the Potential Cost?

Finally, what would be the consequences of different attack types if they did occur? Impact includes operational, financial, and brand damage. Operational disruption, inability to meet SLAs or other customer agreements, and resulting lost customer goodwill are examples of operational impact. Financial impact not only includes lost revenue, lost opportunity, recovery costs, and possible legal costs; it also includes the cost of investment needed to strengthen defenses and mitigate future risk.

Focus on the Material Risks

It is essential to identify material risks. If the potential loss is high, but the likelihood of an incident is very low, it's probably not worth including in your presentation as a significant risk. Knowing where the organization's vulnerabilities lie from a simulation will help you identify what is needed to remedy the gaps. Must current controls be updated and subsequently validated via simulation? Do you need additional or newer technology? Additional staff or expertise, either internal or outsourced?
If you need additional funds, you should support specific investment requests based on the risks they mitigate. Simulations also enable you to quantify how much you can improve the security posture with additional investments.

04 | Spending: Proving the Effectiveness of Security Investments Over Time

Your board likely wants to know: Is the money we are pouring into security investments worth it? Are the IT or security teams actually putting their money where to stop threats and minimize risks?
A clear and quantified view of the infrastructure's most and least vulnerable aspects is key to gauging whether budget, resources, and manpower are indeed assigned where the company needs it most.
An excellent place to start demonstrating the funds' effectiveness would be to share what the cybersecurity team sees as the most vulnerable or exposed potential attack vectors, and, considering the risks associated with that exposure, what resources are allocated to address it.
For example:

- Identifying a high risk of attempted attacks on a consumer-facing application would underline the need to allocate additional resources to harden the WAF (Web Application Firewall).
- A phishing awareness campaign shows that too many employees are clicking on phishing emails, which might indicate the need for additional training.
- An attack emulation shows that a potential attacker could escalate its attack all the way to data extraction, pointing out at insufficient segmentation that needs to be addressed.

Regardless of what the initial assessment indicates, having the technology to measure and quantify the progress achieved between assessments by comparing the success rate of the same attacks and/or increased resilience to a wider number of attacks as a result of the targeted mitigation measures taken is the most effective way to demonstrate the effectiveness of the funds dedicated to cybersecurity.

As the effect of informed, targeted mitigation to maximize the impact is cumulative, the long-term value of investments in cybersecurity grows with time, a result challenging to attain without an extended continuous security validation program.
Over time, a clear global and granular picture of the organization's security investments' impact on your exposure levels and security posture health emerges.

> To demonstrate the effectiveness of funds allocated to digital security, it is imperative to continually record your exposure score.

Valuable benchmarks to report to your board include variance from your baseline. To facilitate this from an operational perspective, any deviation above an acceptable level of risk can trigger an alert, so you are notified of security posture drift immediately.
For example, an exposure score of 20 out of 100, which presents a low risk, can be set as your baseline. Any deviation above that score could trigger a notification to you or your board.
No less important, an executive report can provide your board with a comparison of how your company measures up against other companies in the same industry across the different vectors of the kill chain.

About Cymulate

Cymulate was established with the vision of empowering security professionals to make better decisions faster, based on real-time data.
Founded and led by an elite team of cyber researchers with world-class experience in offensive cyber solutions, Cymulate is determined to become the golden standard for security professionals and leaders to know, control, and optimize their cybersecurity posture end to end. Trusted by hundreds of companies worldwide, Cymulate constantly enhances its methods to prepare organizations for any attack scenario or campaign.
With Cymulate, organizations continuously measure security performance in real-time, shore up defenses, and assure operational effectiveness.
Measuring your cybersecurity performance is fundamental towards creating a more secure organization!

Contact us for a live demo, or get started with a free trial

Start Your Free Trial

05 Appendix A: Sources

- Accenture – 2021 - State of Cybersecurity Resilience 2021: How aligning security and the business creates cyber resilience - https://www.accenture.com/_acnmedia/PDF-165/Accenture-State-Of-Cybersecurity-2021.pdf
- CISA – 2021 - CONTINUOUS DIAGNOSTICS AND MITIGATION PROGRAM Technical Capabilities Version 2.4 Volume Two: Requirements Catalog August 2021 Cybersecurity and Infrastructure Security Agency - https://www.gsa.gov/cdnstatic/Integrated_Technology_Services/CDM-PROG-2021-CDM%20Technical%20Volume%202_v24.pdf
- ENISA (European Network and Information Security Agency) – 2022 – Foresight challenges Report - https://www.enisa.europa.eu/publications/foresight-challenges
- Enterprise Research Group – 2021 - Research Report: The Life and Times of Cybersecurity Professionals 2021 - https://www.esg-global.com/hubfs/ESG-ISSA-Research-Report-Life-of-Cybersecurity-Professionals-Jul-2021.pdf
- Ernst & Young – 2021 - How cybersecurity risk disclosures and oversight are evolving in 2021 - https://www.ey.com/en_us/board-matters/cybersecurity-risk-disclosures-and-oversight
- European Commission – 2021 - The EU Cybersecurity Act - https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act
- Harvard Business Review – 2021 - Risk Management - The SEC Is Serious About Cybersecurity. Is Your Company? - https://hbr.org/2021/09/the-sec-is-serious-about-cybersecurity-is-your-company
- Ponemon – 2021 - Cost of a Data Breach Report 2021 - https://www.ibm.com/downloads/cas/OJDVQGRY
- USA Congress – 2021 - K-12 Cybersecurity Act of 2021 - https://www.congress.gov/bill/117th-congress/senate-bill/1917/all-info
- White House – 2021 - FACT SHEET: President Signs Executive Order Charting New Course to Improve the Nation’s Cybersecurity and Protect Federal Government Networks - https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/12/fact-sheet-president-signs-executive-order-charting-new-course-to-improve-the-nations-cybersecurity-and-protect-federal-government-networks/
- White House – 2021 – Memo: What We Urge You To DATE: June 2, 2021 Do To Protect Against The Threat of Ransomware - https://www.whitehouse.gov/wp-content/uploads/2021/06/Memo-What-We-Urge-You-To-Do-To-Protect-Against-The-Threat-of-Ransomware.pdf
- White House – 2021 – FACT SHEET: Biden Administration Announces Further Actions to Protect US Critical Infrastructure - https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/fact-sheet-biden-administration-announces-further-actions-to-protect-u-s-critical-infrastructure/