ADVANCED CYBER SECURITY CENTER

Survey: Cyber Risk Reporting Challenges and Opportunities

Cyber Risk Governance Program

Briefing Summary

August 2023

In partnership with:

CyberSaint SECURITY

TRUSTED NETWORKS.
ADVANCING CYBER STRATEGIES.

Introduction

The Advanced Cyber Security Center (ACSC) and CyberSaint, a leading cybersecurity risk management software company, partnered to conduct a comprehensive research study aimed at gaining insight into the dynamics of cyber risk reporting in large enterprises. The goal was to understand the current state of cyber risk reporting practices and identify key challenges and opportunities for improvement.

The survey covered a range of topics, including board interest in cyber risk management, the effectiveness of existing cyber risk reporting practices, and changes in the frequency of cyber risk reporting.

Overall, the research conducted by the ACSC and CyberSaint provides valuable insights into the challenges and opportunities of cyber risk reporting in large enterprises. By identifying best practices and highlighting areas for improvement, the research can help organizations enhance their cyber risk reporting practices and better protect themselves against cyber threats. This report will explain the results of the survey, provide additional commentary by industry thought leaders, and provide recommendations on how to improve cyber risk reporting for large enterprises.

Drivers for Cyber Risk Posture Reporting

Cyber risk posture reporting has become an essential component of executing proper cyber risk management in the digital age. The drivers are formidable:

- **Astronomical cost of cybercrime.** According to a report by Cybersecurity Ventures, cybercrime is expected to cost the world $10.5 trillion annually by 2025, highlighting the significant financial and reputational costs of cyber risk incidents, the frequency and severity of cyber attacks, and the importance of effective cyber risk management to protect against cyber threats.

- **Increasing regulatory pressures.** Regulatory agencies around the world are pushing for best-in-class cyber risk reporting to ensure that organizations are meeting regulatory requirements and managing cyber risks effectively. In the United States, the SEC has been at the forefront of this push, requiring public companies to disclose their cybersecurity risks and incidents in their financial filings. The SEC has also issued guidelines for companies to disclose cybersecurity risks and incidents to investors and has emphasized the need for regular cyber risk reporting to board and executive leadership.

- **Investor demands.** In addition to regulatory pressures, there is a growing demand from investors and other stakeholders for organizations to report on their cyber risk posture. Investors are increasingly interested in understanding the cybersecurity risks that companies face and how they are managing those risks. Failure to disclose cybersecurity risks and incidents can result in reputation damage and legal liabilities, making cyber risk reporting an essential component of an enterprise's risk management approach.

- **Attack surface complexity.** The importance of cyber risk reporting is further amplified by the increasing complexity of cyber threats and the growing reliance on technology in business operations. The rapid adoption of cloud-based technologies and the Internet of Things (IoT) has led to more complex IT environments. As well, the COVID-19 pandemic fundamentally changed the level of remote work for many organizations. This added complexity has made it more challenging to manage cyber risks effectively, making cyber risk reporting even more critical.

Cyber Risk Reporting Challenges

Despite the obvious need, reporting cyber risk posture up to the Board of Directors or executives can present significant challenges:

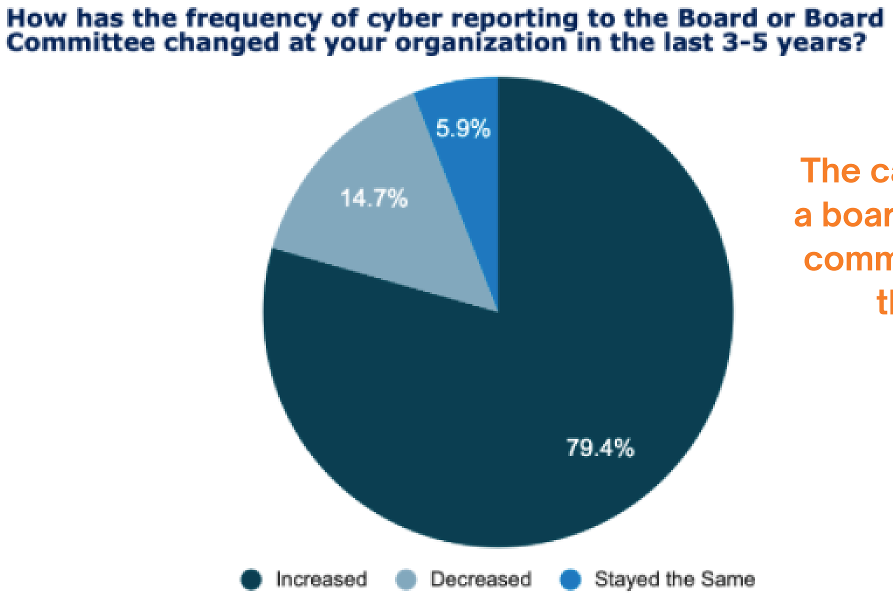
- **Technical complexity.** Cyber risk reporting often involves highly technical information and terminology that can be difficult for non-technical stakeholders to understand. Board members and executives may not have the technical expertise to fully comprehend the implications of cybersecurity risks, which can make it challenging to communicate the importance of cyber risk management effectively.

- **Lack of standardization.** Cyber risk reporting practices can vary widely across organizations, making it difficult to establish consistent reporting metrics and benchmarks. This lack of standardization can make it challenging to compare cybersecurity performance across different business units or industry peers, which is a long-desired aspiration of the industry.

- **Reporting time, expertise and cost.** Cyber risk reporting can be resource-intensive, requiring time and expertise, and even the largest organizations often resort to spreadsheets and powerpoint presentations to attempt to measure and report upwards. This method only provides a point-in-time view that is often based on stale data, and takes significant time and resources, leading to incomplete or inaccurate reporting.

Research Study Findings

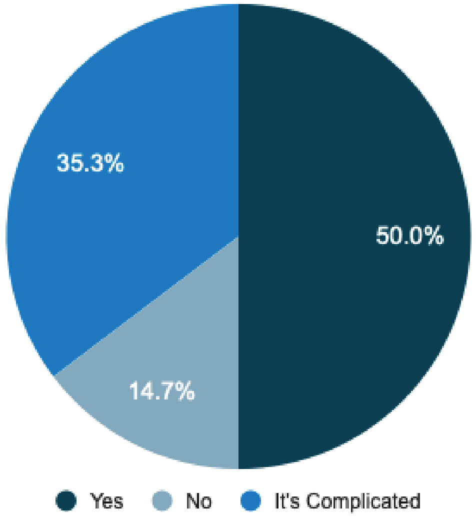
The Advanced Cyber Security Center and CyberSaint set out to assess current cyber risk reporting practices amongst the ACSC membership. Thirty Chief Risk Officers, Chief Legal Counsels, and Chief Information Officers from ACSC enterprises - across verticals including finance, healthcare, and energy - were surveyed to gain insight into cyber risk reporting trends. Survey responses are shown below:


How has the frequency of cyber reporting to the Board or Board Committee changed at your organization in the last 3-5 years?

The cadence of reporting to a board of directors or board committee has increased in the past 3-5 years.

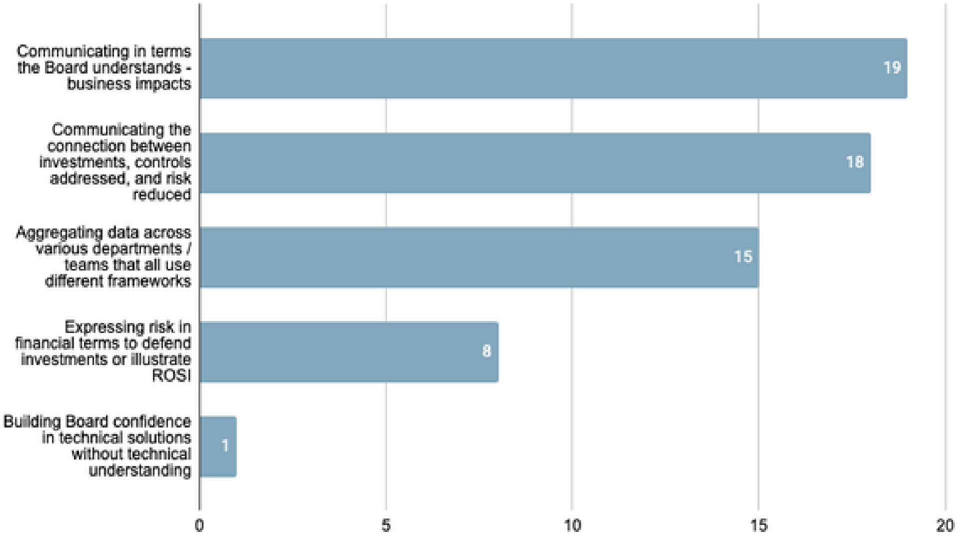
ADVANCED
CYBER
SECURITY
CENTER

Do you have a CEO-led council of senior executives that oversees cybersecurity and meets 2+ times per year?



Half of the respondents have a council overseeing cybersecurity that meets 2+ times per year.

What are your top two challenges when reporting on your cybersecurity posture to the Board or upper management?



Communicating in terms the Board understands circa how cyber impacts the business, and communicating the connection between investments, controls, and cyber risks are the top challenges.

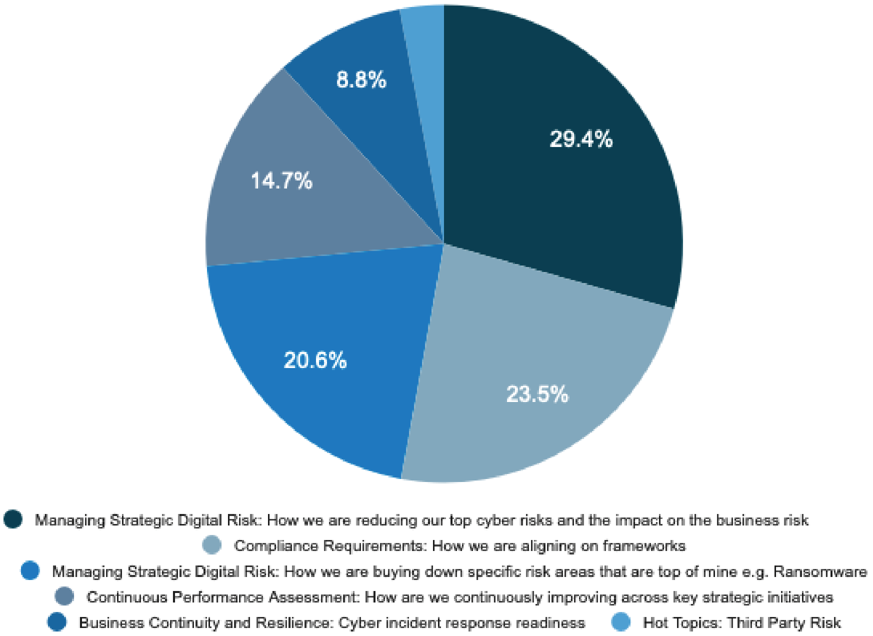
Contact us

(617) 584-0581

jdinneen@acscenter.org

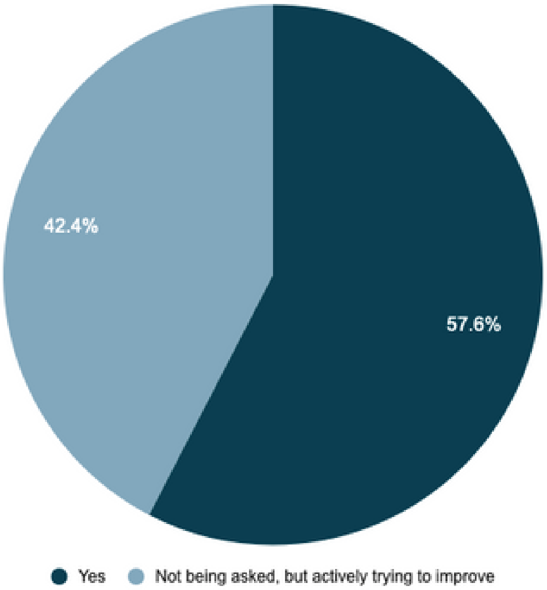
ADVANCED CYBER SECURITY CENTER

What is the top priority from the Board or upper management for your cybersecurity program today? In other words, what do they care about the most?



Respondents' answers varied here, as Board members and executives face many significant priorities. Still, managing strategic digital risk and explaining how the organization is aligned with compliance requirements rise to the top.

Is your Board looking for improvements in cyber risk reporting?



The majority of respondents noted their Board of Directors is looking for improvements in cyber risk reporting. All respondents are actively trying to improve cyber risk reporting.

Contact us

(617) 584-0581

jdinneen@acscenter.org

ADVANCED CYBER SECURITY CENTER

Cyber Risk Board Reporting Best Practices

Comprehensive cyber risk reporting provides needed visibility into an organization's cybersecurity posture, including its top risks, strategic initiatives, and benchmarks compared to industry peers. This information is essential for board and executive leadership to understand the organization's cybersecurity risk exposure and make informed decisions about cybersecurity investments and risk management strategies.

Best practice recommendations from ACSC CISOs, Chief Risk Officers and Legal Counsels:

- **Tailor reports to the audience.** Cyber risk reports should be tailored to the specific audience that will be receiving them. Boards and executive leadership typically require high-level overviews and key performance indicators, without diving deep into technical details. Reports should show easy-to-understand visuals such as trend reports, gap-to-goal graphics aligned with compliance frameworks that are being tracked, and a list of top risks to the organization vs their peers to be discussed.

- **Focus on business outcomes.** Cyber risk reporting should focus on the impact that cybersecurity risks can have on the organization's business outcomes, such as revenue, reputation, and customer trust. This helps to contextualize the risk in terms that are meaningful. One method of mapping cyber risk posture back to business initiatives is to track strategic initiatives and the assets or assessments related to those initiatives. Examples include cyber risk posture of all software applications being sold by a software company, or cyber risk posture by business unit or global division.

- **Provide actionable information.** Cyber risk reporting should include actionable information that enables Board and executive leadership to make informed decisions. Actionable guidance should include effectiveness of current controls, emerging risks, and the potential impact of cyber threats in dollars - all directly material to explaining potential investments versus potential losses.

Contact us

(617) 584-0581

jdinneen@acscenter.org

- **Use a standardized reporting framework.** Standard content formats help ensure consistency and comparability across departments and stakeholders, which reduces the time and effort required to create reports. Common dashboards that cover key concerns of the audience can be immensely beneficial, and risk quantification models that are tailored to the business and used consistently can help explain cyber posture in financial terms that are readily understood.

- **Incorporate risk scenarios.** Risk scenarios that illustrate potential threats and their potential impact help drive decision-making around risk management strategies. This includes what-if scenarios around potential for risks to be mitigated, investment required across people, process, and technology, as well as potential monetary values saved versus lost.

- **Regular interval reporting.** Cyber risk reporting should be conducted on a regular basis to ensure that the Board and executive leadership have accurate and up-to-date information about the organization's cybersecurity posture.

Survey Reinforces ACSC Board Report Findings

The need for effective cyber risk reporting is tightly coupled with key points made throughout the new Advanced Cyber Security Center's (ACSC) report produced by Mass Insight, Leveraging Board Governance For Cybersecurity, Front Line Perspectives on How to Improve the Board / C-Suite Partnership. Strong cyber risk reporting can directly address the very issues that have been slow to improve since the ACSC's 2018 report on cybersecurity governance:

- **Disconnect.** While ACSC CISOs and Risk Officers report progress in their Board's cyber maturity, Board members and advisors from a larger universe of organizations describe a continuing struggle with cybersecurity risk governance. Board members lament they continue to get overly-technical reports from management teams that fail to put governance in business and financial terms. While cyber risk has by all accounts become a higher priority for Boards, security executives are frustrated that too often cyber risk and cyber management continue to be secondary topics to enterprise strategic plans and success.

  - Comprehensive cyber risk reporting is central to elevating the role of the CISO, moving from operational reporting to business risk/impact reporting, and board understanding of cyber issues. Cyber risk quantification methods can help here, when implemented simply and transparently understood.

- **A One-Way Conversation.** From all interviews, only a few examples show evidence of Boards challenging management and changing cyber strategy and practice in ways that the new SEC regulations will require. The discussions largely remain a briefing from CISOs and Risk Officers to Boards. Although this was the case, this is quickly changing as we have experienced more urgency to change in recent conversations with enterprise organizations.
  - Comprehensive cyber risk reporting can underpin the close dialog, understanding, and decision-making that the SEC is imposing upon Boards and executives.

- **Cybersecurity In A Box.** Cybersecurity continues to be dealt with at the Board and Board committee levels as separate and distinct from broader business strategy and risk management. Cyber agenda time for full Boards is restricted to annual meetings, and generally, quarterly Board committee sessions.
  - This is changing as effective cyber risk reporting is moving CISO interactions with the Board front and center, as opposed to a back-room footnote.

- **Frameworks And Metrics.** As we saw four years ago, frameworks that place cyber risk into a larger business context are a work in progress and fall short of what's needed for comprehensive Board cyber risk governance.
  - The very essence of Board and executive level cyber risk reporting is the tip of the spear for all underlying metrics. Get the story right at the highest level and downstream frameworks / metrics will be forced to move from the obtuse or arcane into supporting evidence with distinct clarity.