



Top 5 Cyber Risk Questions Board Members Ask Axio

axio

Executive Summary



Board Members Request Business-Centric Cyber Risk Reporting

Recently, our board member customers have expressed great interest in understanding cyber risk in business terms.

Proactive governance is becoming essential considering the increasing physical and cyber devastation over the past few years. Board reporting is shifting from reliance on a 'defend and protect' mindset to a more capable 'mitigate and manage' methodology.

Axio is honored to serve as the guiding light for board members during this global reset on cybersecurity board reporting. In this article, we will share the top 5 cyber risk questions our board member customers have asked us. We will also explain the significance of these questions and provide an easy-to-understand solution.

The top 5 cyber risk questions board members ask Axio are:

1. Can I view cyber risk beyond a heatmap?
2. How does the emerging threat landscape impact our company?
3. How can I measure the amount of cyber risk reduced over time?
4. How is our organization doing in relation to industry peers?
5. How can I ensure I fulfill my cyber responsibility as a board member?

The answers:

1. Beyond a heatmap:

You can prioritize cyber risk based on financial impact. Boards want to see what the top risk is in financial terms

3. Cyber risk reduction

You can track how the implementation of new control initiatives and reduce exposure and improve cyber program maturity. Boards want to see how much risk is reduced over time in monetary terms, not the same color of risk every quarter

5. Cyber responsibility

You can fulfill your fiduciary responsibility by requesting a cyber-scenario analysis to visualize how much an event can cost in financial and operational terms exclusive to business operations. Afterwards, your organization has the necessary information to prioritize the most necessary steps to reduce risk.

2. Threat landscape view

You can determine the impact of emerging threats by performing a cyber risk scenario analysis. Boards want to focus on scenarios that have financial and operational relevance to their business

4. Peer benchmarking


You can use the Axio360 platform's unique data-driven benchmarking capabilities to see how the security organization is performing in relation to industry peers and competitors.

Boards want a source of objectivity and motivation to determine if the organization is below or above our risk appetite and risk tolerance in order to prioritize budget and human capital

Free advisory consultation for board members

Learn how Axio gives board members more valuable cybersecurity reporting

sales@axio.com



If you read the minutes from just about any zoom board meeting in 2020, you'd find similarities in tone, often hinting of a panic, the kangaroo word of the overarching problem: pandemic.

Introduction

Why Boards are Prioritizing Cyber Risk in 2021

It's hard to disagree that 2020 was a dark time for board members. The board room remained mostly unoccupied, replaced by a collection of digital zoom squares. Happy hour was more about describing the drink of choice from a socially accepted digital distance than actually tasting it.

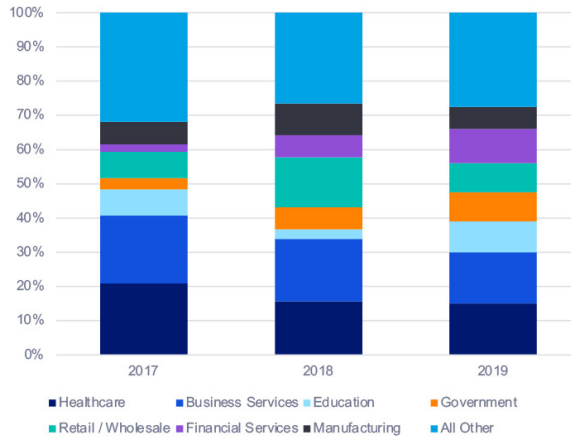
Board conversations centered around ensuring business continuity and servicing customers without interruption. Despite a global lockdown, certain industries thrived, such as e-commerce and home improvement. Unfortunately, others had to scramble to adapt to digital-first touchpoints. Business models were reinvented overnight, and many sacrifices were made by both executive leadership and staff employees.

During this above-described corporate pandemonium, board members suddenly faced an additional new and prioritized risk: the increased likelihood of a successful cyber-attack. In particular, no industry or sector was immune to ransomware, which became the #1 cyber risk on every security professional's mind.

Ransomware is democratic and expensive

- No industry sector or geography is immune; attackers are opportunistic.
- Initial ransom demands now approach ~\$40M; with the average drifting up dramatically in 2020 to >\$8M.

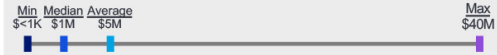
Global Ransomware Claims by Industry



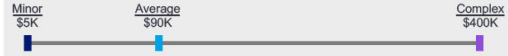
AIG data as of Q2, 2020

Ransomware Financial Impacts

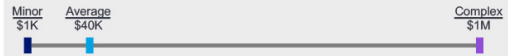
First Ransom Demand – 2016 – 2020



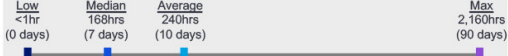
Incident Response Fee Range – Survey of Major Providers



Breach Counsel Fee Range – Survey of Major Providers




Business Interruption Length – 2016 – 2020



A New Year's Ransomware Resolution.

Presented digitally at Security Boulevard by Axio President Dave White and AIG's Cyber Product Leader, Garin Pace.

This [presentation](#) shows how to address ransomware risk in 2021 by using the proprietary Axio360 ransomware assessment methodology. Currently the model and its reporting output are free as a single-user license in Axio360. Axio welcomes interested professionals to test drive our platform's exclusive risk management capabilities and schedule a brief discussion to discuss particular use cases.



The following is an abstract depiction of invisible threat groups (cybercriminals + nation states). Attribution may or not be representative of external cultural markers.

A Threat Impossible to Identify

Board members continued to be bombarded with unpleasant news of cyber-events in 2020.

As most of the world continued to work from home, cybercriminals took advantage and attack attempts increased by 400% according to the FBI.

By the end of 2020, the SolarWinds crisis, a monster of a cyber risk scenario, stepped out of the shadows, rearing its ugly head. Hackers operated sight unseen for many months by exploiting a creative supply chain vulnerability, and it was only discovered many months later. By then the damage was done. This ingenious

attack vector was the brainchild of a new type of adversary, one that combined the brightest cybercriminal minds with the unlimited resources of a nation state.

Working together, they were impossible to identify by traditional detection technology. We call these new actors invisible persistent threat groups.

2021 shows no signs of a cyber peace treaty. Boards are eager to extract more value from cybersecurity reporting and view relevant risks through a context specific to their unique business operations.

The Top 5 Questions Board Members Ask Axio

1. Is it possible to view cyber risk beyond a heatmap?

Presenting risk in colors is an acceptable and recognized reporting output at many enterprises

Heatmaps provide comfortable visual representations, easy to discuss in a limited time frame. However, heatmaps usually do not disclose financial indicators for boards to measure and track progress or to stack rank cyber risks based on calculated loss exposure.

Why is understanding loss exposure in dollar amounts necessary in 2021? Because it's much more meaningful information in these times of inevitable attacks. Qualitative reports only provide a rudimentary snapshot of a corporation's cyber health. Imagine a doctor checking only 3 basic things to calculate your risk for a medical condition: heart rate, blood-pressure, and breathing. Without taking a blood sample for more accurate markers, it's impossible to make an educated determination of what's at risk.

We've spoken to board members who told us a certain type of risks can remain the color yellow for many reporting periods. This leaves them playing a guessing game of "what's changed?" and "how are we doing in relation to last quarter?"



In Axio's [presentation](#) on cyber risk quantification, co-founder and President David White discusses interactions boards have with CISOs, and the reporting roadblocks heatmaps can present.

We are not arguing that heat maps should be abandoned entirely, as they do have a useful place in business reporting and can help push a shift in business culture. However, cyber risk information is much more valuable once it's prioritized based on financial impact in relation to the business as a whole. In this way, a board member can quickly compare and contrast what areas of the business are more susceptible to a cyber-event and understand what actions can be done today to decrease the risk.

2. How does the emerging threat landscape impact our company?

Our board member customers have storied careers in business spanning many decades. They did not get to their positions by standing in the sidelines and ignoring emerging threats and risks, often publicized in the news and media.

No risk landscape has changed as dramatically as the digital one.

Connected devices and cloud adoption have made the digital perimeter impossible to define and protect. The internet is now a complex multi-faceted surface with new dimensions and layers. A cyber-attack is no longer just the theft or destruction of data, it's about protecting human and corporate existence. Only a few months ago, a hacker was successful in accessing an internet-connected control system for a water treatment facility. Fortunately, an IT operations employee was able to quickly reverse the malicious control system instructions and prevent an entire county from drinking toxic water.

Every time a new event is publicized in the news, board members ask, "How does this affect us?" And the word **us** is hyper focused on the business as a whole.

Some common scenarios boards are concerned about include:

- Attacks on third-party vendors over which control and visibility is limited.
- Ransomware on control systems for manufacturing and IoT or medical devices.
- Attacks on connected critical infrastructure control systems.

Fortunately, any cyber scenario can be represented as a best- and worst-case outcome, in dollars and cents. The security industry often refers this approach as cyber risk quantification. There are multiple methods of approaching this objective. We recommend that board members select a process that is dynamic and continuous, allowing them to reassess their risk as conditions change.

Some common scenarios boards are concerned about include:

At Axio, our platform allows quantification to be **done in as little as 1 day** (leveraging a built-in scenario library and easy to understand formulas). The quantification of a cyber scenario can be described in three simple steps:

- Devise scenarios, document assumptions, and which business functions would be impacted (or pick from Axio's built-in library).
- Prioritize the scenarios by highest business impact, taking into account existing controls, program maturity, and planned control initiatives.
- Estimate the financial and operational impact of each risk scenario

The output of this process can provide immediate value and is easy to refine.

If you're interested in learning the limitations of other quantification methods, particularly ones that are grounded in estimating probability of a threat materializing against an asset, we have a factsheet titled, [Probability vs Priority](#) we highly recommend checking out.

Identifying the expected financial loss range of identified and emerging cyber risks allows board members to sleep better at night. Once calculated, the risk can either be **accepted** as not particularly impactful, **transferred** to an insurance policy, or **reduced** through people, process, and technology controls.

In summary, realistic cyber risk quantification allows board members to understand what risks need to be prioritized for action in order protect the crown jewels of the company.

3. How much cyber risk was reduced last quarter?

Continuing the conversation about risk reduction from the previous section, we admit this is a new trend in board reporting.

Traditionally, when a CISO reports on the current state of cybersecurity, board members often ask about budget and progress of the program. The budget is usually given as a simple top-line number needed to accomplish a group of technology initiatives, remain in compliance or close audit findings. Cyber risks are often shown on a heatmap using red, yellow, or green boxes or a numerical scale of 1-3 or 1-5 but there often is no rationale as to why a certain risk is in a certain box, number or color.

In regard to the maturity of the program and compliance to regulations (which often go hand in hand), board members also receive a report with a score or rating, as well as a summary of identified gaps. The rating or score can be calculated by using a multitude of frameworks and models. You can learn about which cybersecurity framework is right for your needs by viewing our recent presentation.*

Useful tip: You may need more than one cybersecurity framework for your particular needs.



Behind every successful cybersecurity program is a framework. In 2021, there are dozens of models and standards to consider, as well as potential regulations to comply with. Given the growing complexity of both digital and physical risks, we are often asked, "Which cybersecurity framework should I use? Should I use more than one? And if I use more than one, how do I do that in a way that I can get maximum value?"

Returning to risk reduction, board members are now desiring this information in business language. It's much more valuable to make decisions based on the financial or operational impact rather than a group of colors or an arbitrary score.

The transition point came when organizations realized they were spending millions upon millions on various cybersecurity initiatives and continued to be hacked. Not only did the events have repercussions that extended to business operations, but they demonstrated how current board reporting often didn't provide insight into how much was at stake to begin with. It's very simple to understand how much risk can be reduced for a particular cyber scenario. In the Axio360 platform, the Control Initiatives feature allows one to select and model the desired controls for improvement and see how they can reduce the risk.

This can be reported quarter over quarter to show how actual controls made a reduction in the overall risk exposure by application of appropriate resources. Board members can finally have a more data-driven view of risk reduction in dollars and cents.

4. Where can I see how our organization's cyber posture is in relation to our peers?

Improving cybersecurity posture is a journey. At Axio we believe cybersecurity assessments are a process of continuous improvement over time.

Just like someone on a fitness plan will not turn into a bodybuilder overnight, an organization must tackle their gaps and deficiencies realistically. And just like you don't get fit from one workout in the gym, you can't stop improving cybersecurity after implementing certain controls or meeting a compliance requirement.

Regardless of what cybersecurity framework an organization uses: NIST CSF, C2M2, CIS20, and countless others, a perfect score is not only challenging actually but may be unnecessary. Continuing on the theme of this article, a risk-based approach to cybersecurity focuses less on the completeness of certain controls or compliance frameworks and more on how the associated risks would impact the business if realized.

5. How can I fulfill my fiduciary responsibility when everything's at stake?

As cyber threats continue to morph and grow, society is beginning to require greater accountability from the boards and senior leaders of the companies we trust with our information.

Being a board member may soon become a risk in itself if one doesn't have the proper information to make security decisions. Considering [the recent Capital One breach](#) and the shareholder class-action lawsuit, it's possible that after this litigation, the government may pass cybersecurity legislation to prevent repeat events.

Board members need better information about all risk types to make executive decisions. While assessments on compliance and maturity are excellent instruments to understand present state, as well as provide a score to track improvement, they are only one piece of the reporting puzzle. Board members need to have a future outlook as well, [understand the risk scenarios pertinent to their business and the greater landscape.](#)

The only way to look to the future is by aligning cybersecurity to the financial statements of the organization. With a cyber risk quantification process, informed by program maturity, control initiatives, risk scenario quantification, and insurance portfolio analysis, board members can rapidly determine which scenarios are critical to address.

Conclusion

The Boards Must Empower the CISO, and Vice Versa

Cybersecurity leaders such as CISOs are now being analyzed not only under a governance microscope but placed inside a pressure cooker

Suddenly, cybersecurity is the top business risk for board members to understand. There's a desire to become an immediate expert without years of experience and training.

CISOs are being tasked with presenting a defensible report to the board that makes business sense to a C-level audience. The analysis must now be more than just a codification of a color spectrum representing various risk levels but have financial and operational indicators that tie back to the organization's strategy and mission.

This shift in board member thinking is continuing to evolve. Our professional services team works with many respected security leaders of Fortune 100 organizations with responsibilities that get rolled up into board reporting. Some common measurements include: the reduction or transfer of risk, compliance, requesting new technology budget, and ultimately reporting cybersecurity posture. However, these initiatives are often siloed and do not reflect how

they all relate to business as a whole. If the desired outcome is to unify cybersecurity and business, the reporting has to change. We can help. Axio360 reporting can help CISOs demonstrate measurable progress. The platform also allows CISOs to have a ground truth for their control initiatives, which if planned properly can demonstrate clear value to the organization and justify often costly security and privacy initiatives.

Some greater CISO benefits beyond just better board reporting include:

- Making the security team more productive and the central communicator of cyber risk as a business function instead of strictly a technology initiative.
- Building stronger relationships with suppliers and vendors by demonstrating control initiatives to reduce risk.
- Empower entry into new markets and acquire customers that are highly regulated and require a higher standard of controls implemented.
- Eliminate duplicate controls and technology redundancies resulting in cost savings.
- Optimize the insurance portfolio premiums by demonstration of certain control implemented and their effect on risk reduction.

Axio is here to lead the way with the an integrated risk management platform that is used by many sectors of our critical infrastructure and was ranked by Gartner as a Cool Vendor in 2020 Axio's mission is to help organizations understand their unique cyber scenarios in financial and operational terms to make data-driven and informed business decisions

Curious about how we do it?

[Schedule a brief conversation](#) with one of our experts and get instant access to our free single-user assessment toolkit. You can enjoy benefits of being part of the Axio community and learn the very latest on how we are taking charge on a risk-based approach to cybersecurity.