



axio

Making the Business Case for Cybersecurity Investment



Quantify cyber risk with transparency and actionability.

Table of Contents

3. Executive Summary

6. The Axio Cyber Risk Quantification Method

Identify Mission-Central Parts of the Business That Could Be Impacted by a Cyber Event

Analyze the Financial Impact of Plausible Cyber Events

Optimize the Entire Portfolio of Controls

Manage Cyber Risk on an Ongoing Basis

20. Axio Makes Cyber Risk Quantification Accessible

22. About Axio


Executive Summary

Organizations are using outdated, unreliable approaches to cyber risk management. These approaches are proving insufficient. **Here's why.**

Companies that measure cyber risk using “high, medium, low,” or “red, yellow, green” have essentially no visibility into their real financial exposure.

Such qualitative approaches do not give CEOs the information they need to know how and where to invest to minimize their risk effectively. And these antiquated methods do not generate defensible outcomes.

CEOs and cyber leaders need an approach to cyber risk management that helps them decide what cyber controls—financial, technical, physical, administrative—to prioritize and invest in and when it makes financial sense to accept risk. The only way for organizations to understand how cyber events could impact their bottom line is by calculating the financial costs of, or quantifying, their risk. Today, most organizations are not quantifying what a security incident would cost them.ⁱ



There is a dangerous disconnect between CEOs and cyber executives.

Cyber executives aren't framing risk in a way CEOs and others in the C-suite understand. This means CEOs are not fully comprehending what cyber leaders are saying—and poor or uninformed decision making is happening.

High-profile cyberattacks in recent years, such as the infamous Equifax data breach when hackers stole the information of 147 million Americans in 2017,ⁱⁱ highlight what can happen when CEOs and cyber leaders aren't in sync. Research firm Gartner analyzed the former Equifax CEO's congressional testimony regarding the incident and found “a disconnect between executive understanding and levels of cybersecurity capabilities in the organization.”ⁱⁱⁱ

To solve this problem, cybersecurity executives must talk to CEOs and other executives in a language they understand—business terms. And to do this, they need to know the financial impact of cyber risk—they need to quantify it. By quantifying the company's cyber risk, security leaders will have the information they need to show the CEO and the C-suite how an incident could impact major business areas such as logistics, reputation, and legal.

Boards are frustrated—tired of fear and uncertainty. And they are not holding back when it comes to changing out leadership after cyber events. Equifax is far from the only example. Breaches over the past several years have seen the CEOs, CIOs, and CISOs of major companies, including Target, Sony Pictures, and Capital One, among many others, leave their prominent posts. There is also growing pressure on boards. Regulations in Europe and the U.S. are tighter.

Moody's has started incorporating a company's risk of a major cyber attack into its existing credit ratings. And the SEC has updated cybersecurity disclosure guidance, now imploring companies to disclose their understanding of cyber risk versus just disclosing events after the fact. For boards to follow their fiduciary duty, they need a clear picture of the company's cyber risk—in business terms.



Cyber leaders must start quantifying cyber risk. Axio's unique method is transparent, efficient, actionable—and **approachable.**

Axio's cyber risk quantification method and the SaaS platform that powers it, described in this paper, give companies the tools they need to determine how to guard against losses today and plan for how to protect their operations tomorrow. Axio's method follows a straightforward four-part process:

- **Identify** mission-central parts of the business that could be impacted by a cyber event
- **Analyze** the financial impact of plausible cyber events
- **Optimize** the entire portfolio of controls
- **Manage** cyber risk on an ongoing basis

The Axio Cyber Risk Quantification Method

Identify Mission-Central Parts of the Business That Could Be Impacted by a Cyber Event

The Axio process starts with the identification of a company's essential functions—the things that keep the lights on and business flowing that could be impacted by a cyber event.

By identifying what is most important to achieving the company's mission and creating value for customers, stakeholders will be able to narrow down the people, processes, and technology they need to focus on. This business-value centric approach also ensures that team members from across the company play a role in managing cyber risk.

Instead of a sole cybersecurity or IT department putting controls in place, leaders from every unit weigh in on what business operations—and outcomes—the company needs to prioritize. The shift from subjective risk ratings owned by the cybersecurity team to business-centric risk analysis with broad stakeholder involvement is a major change. Axio and its partners provide advisory services to help make that change.



Next, stakeholders determine plausible cyber incidents that could disrupt or destroy the underlying technical infrastructure that supports the essential business operations and assets they identified. Insiders who understand a company's dependence on technology are best equipped to identify cyber risks that would seriously impair critical business functions.

Stakeholders may begin with a simple scenario such as "We could get ransomware." And then move into more nuanced situations.

For example: "Attackers could slightly alter the chemical mix for this key product component, which would lead to quality issues that we might not discover until units start failing at customer premises."

The goal is for stakeholders to determine the primary ways a hacker could use technology to steal from a company or disrupt its business through targeted or opportunistic attacks.



Axio's professional services team leverages insights from the platform's user community for a **comprehensive view of risk scenarios.**

Stakeholders need to validate that enough scenarios exist and represent all essential areas of the business. Axio's easy-to-use SaaS platform, Axio360, helps users see where they have gaps through a simple grid. This chart shows the business units that stakeholders already identified in their cyber event scenario brainstorming process and how many scenarios they have generated.

Once stakeholders identify enough cyber event scenarios to be representative of the risks their business is facing, they use Axio360 to enter high-level descriptive information for the scenarios and set up a susceptibility rating. They include enough information to be able to prioritize which scenarios they want to analyze further.

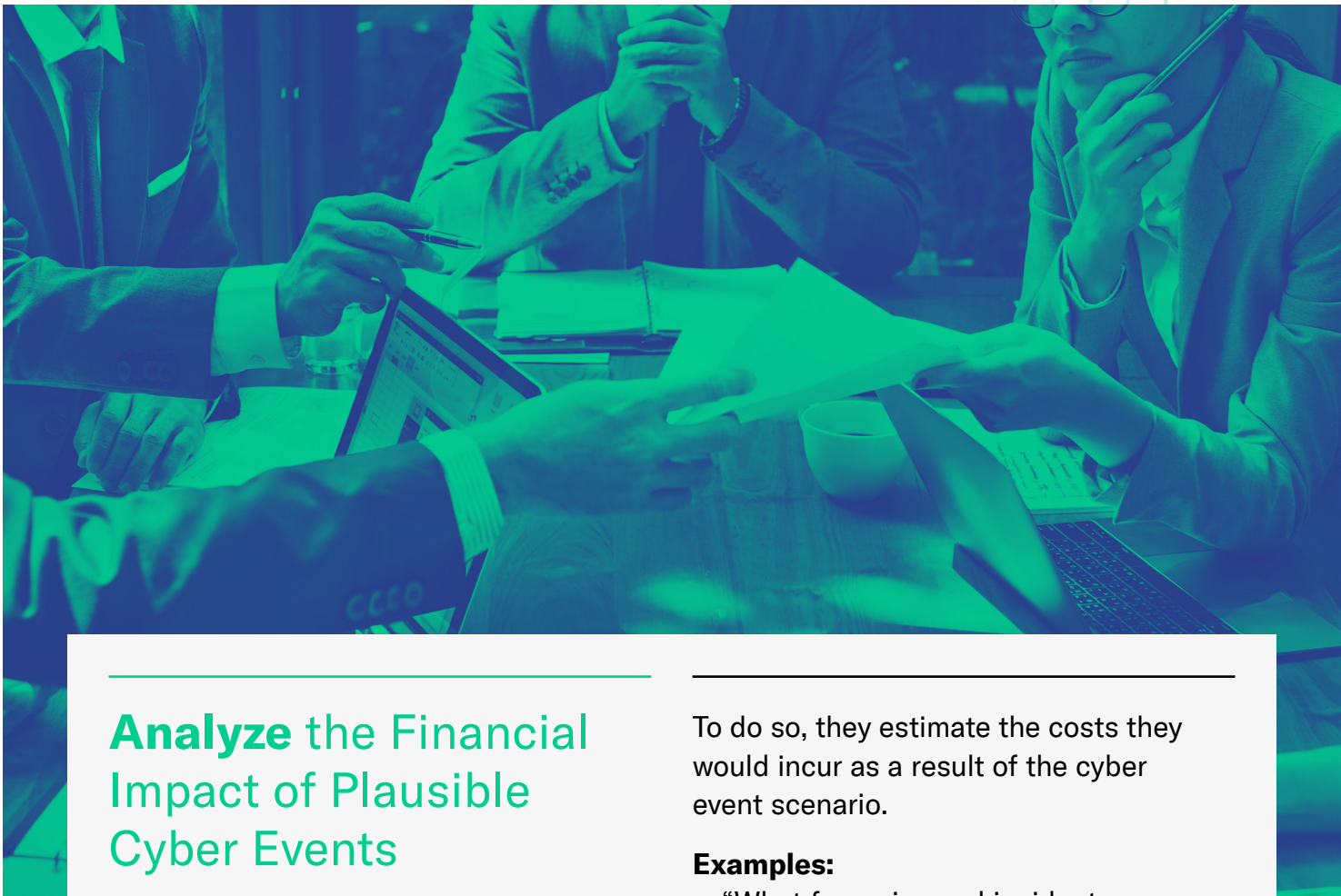
This is an example summary: "We could experience a ransomware event in our most profitable factory during our peak production period, leading to downtime of more than two weeks. This would result in our inability to meet market demand for our top-selling seasonal product, leading to poor financial performance for the year and reduced share price. We rate our susceptibility to this event as medium-high because we have poorly performing software patching at this location."

Businesses can also overlay assumptions in the high-level summary. For example, company security leaders could say: "We are assuming in the scenario that the cyberattack will only impact one plant. It isn't going to happen at all of our plants because the plants aren't connected." The security leaders would then know that they aren't trying to model a coordinated attack on the company.

By grounding the scenarios in enough context, stakeholders will have the information they need to prioritize which scenarios they need to focus on for financial analysis and accurately estimate the financial impact of cyber events.



The Axio process
helps companies find
their **blind spots**.



Analyze the Financial Impact of Plausible Cyber Events

Stakeholders are now ready to analyze the financial impact of these plausible cyber events on their business.

To do so, they estimate the costs they would incur as a result of the cyber event scenario.

Examples:

- “What forensics and incident response costs are we likely to incur?”
- “What will be the cost to restore damaged data?”
- “Are there regulatory fines that will be imposed upon us?”
- “What revenue will we lose due to business interruption?”
- “How much will we need to pay in penalties because we didn’t meet contract obligations?”
- “What is the amount of loss due to physical damage to machinery and equipment as a result of the incident?”
- “What legal fees would be incurred due to a shareholder class action suit related to the incident?”

Stakeholders can then create formulas, use Axio's pre-built formulas, or enter lump-sum ranges to estimate the financial impact of the cyber event. For example, in a scenario in which a cyber event disrupts a factory that produces a just-in-time supply chain component, the company might think through:

- “How many days would it take for us to resume production?” The business may estimate 10 to 20 production days lost.
- “How many days of product do we have in inventory?” Inventory availability could be confirmed to be 5 days.
- “What is our contractual penalty for late delivery of the product?” Product managers could assume a range of penalties of \$600,000 to \$800,000 per day of delay, depending on the customer being impacted.
- Resulting in an impact estimate of ([Production days lost: 10 to 20] – [Days of inventory: 5]) * [Penalty per day: \$600k to \$800k] = \$3 million to \$12 million in impact.



AXIO360 Formulas

Axio360 offers a set of core impact types from which to choose, and users can easily add custom impact types. The core impact types cover essential classes of impact, such as forensics, data restoration, and lost business income.

Axio360 includes a library of formulas, one or more for each core impact type. Alternatively, users can enter custom formulas. Formulas are shown in natural language form to make the impact estimate completely transparent.

For each component of a formula, users can set the minimum, estimated (most likely), and maximum value. Entering this set of numbers allows Axio360 to calculate an impact distribution using Monte Carlo simulations.

Axio360 also provides suggested values for the standard formulas. Suggested formulas and values are based on expert research and machine learning.

Axio360 allows users to set whether each estimated value applies to the entire company or just a specific scenario. This allows commonly used values such as hourly legal rates to be leveraged across all scenarios and adjusted centrally.





Axio's method for having companies control the formulas and values for every single impact ensures that stakeholders have complete transparency—and, importantly, means that each impact is directly tied to the bottom line. By connecting cyber events to financial impacts, Axio helps companies make business decisions, including:

- Deciding about insurance purchases
- Taking calculated risks in adopting new/emerging technology
- Making acquisitions
- Going into joint ventures
- Creating policy changes
- Investing in new cybersecurity controls
- Determining divestment decisions



This process allows users to own every single input—giving them **complete transparency**.

After estimating the impacts for all scenarios, Axio360 makes the calculations and visualizes the financial summary for review. Understanding the financial impact frames cyber risk as a business problem and enables action. What can we do to minimize potential impact? How can we reduce our susceptibility? And do we have enough financial capacity to endure the event? These are critical next questions that spawn action.

	First-Party Impacts	Third-Party Impacts
Financial Impact	Your Income and Expenses 	Others' Income and Expenses 
Tangible Impact	Your People, Property, and Environment 	Others' People, Property, and Environment 

Axio360 buckets each impact in a scenario into one of the **Axio Quadrants**.

Axio utilizes a quadrant system that categorizes costs by:

- **First-party financial impacts**
(money a company could lose)
- **Third-party financial impacts**
(money another party could lose)
- **First-party tangible impacts**
(a company's physical property and employees that could be affected)
- **Third-party tangible impacts**
(another party's physical property and employees that could be affected)

Axio provides businesses with the core types of impact for each quadrant.

These include forensics, data restoration, and personal injury, among others. The Axio Quadrants take a comprehensive view of losses, including not just the direct and immediate consequences of a cyber event, but also the ongoing effects on business operations and income generation.



For example, if a business is developing a ransomware attack scenario in Axio360, the company will consider the direct costs of incident response and data restoration as well as all costs for forensics, public relations, legal advice, regulatory filings, lost income from the outage, lost income from reputation damage, defense costs, and litigation costs.

	First-Party Impacts	Third-Party Impacts
Financial Impact	Response costs such as forensics, notifications, and credit monitoring Legal expenses such as advice and regulatory filings Lost income from network or computer outages, including cloud Theft of funds, monies, or securities Cost of restoring lost data Cyber extortion expenses Value of stolen intellectual property Other financial damages	Consequential lost income Restoration expenses Legal defense Civil fines and penalties Shareholder losses Other financial damages
Tangible Impact	Mechanical breakdown of your equipment Destruction or damage to your facilities or other property Environmental cleanup of your property Lost income from physical damage to your (or dependent) equipment or facilities (business interruption) Bodily injury to your employees Other tangible damages	Mechanical breakdown of others' equipment Destruction or damage to others' facilities or other property Environmental cleanup of others' property Bodily injury to others Product liability Product recall expenses Other tangible damages



Businesses can review the individual elements driving the overall cost of their cyber risk. This granular approach enables cybersecurity leaders to justify each value to their CEOs and boards.

First-Party Financial Impact Example:

 Impact	 Assumption	 Estimate
Response costs such as forensics, notifications, and credit monitoring	Forensics Team Hourly Rate (\$250-\$600) * Forensics Team Weeks (5) * Forensics Team Size (4) * Forensics Team Hours Per Week (60)	\$300,000 - \$720,000



Chemical manufacturer uncovers **major cyber exposure**

A large, publicly traded chemical manufacturer had an overflow protection system in several chemical manufacturing plants that required three engineers to monitor and adjust various manual controls continually.

The leadership decided to eliminate the jobs of those engineers (and thus their salaries) in favor of computer-controlled automatic valves—a **few hundred thousand dollars in annual savings.**

Before executives made that decision, when the three engineers were still employed, a cyberattack would have been impossible to carry out because the manual fail-safe valves would have protected the plants. With computer-controlled automatic valves, a hacker could disable the valves, overfilling the tanks and damaging the plant, **costing more than \$800 million in losses.**



Once the company learned about this exposure by going through the Axio process, **it reversed its decision and rehired the three engineers.**



Optimize the Entire Portfolio of Controls

Axio's unique Control Initiatives method helps stakeholders optimize their entire portfolio of controls—financial, technical, physical, and administrative.

The Control Initiatives method allows companies to play out how changing one or more controls would affect their exposure. Stakeholders can evaluate how much of the risk that is inherent to a cyber loss scenario they could reduce by changing a control, and they can consider how much additional risk they would be taking on if they were to reduce their controls.

To test the impact of a new control, the stakeholders just change any variables (e.g. number of computers) that the new control (or set of controls) would affect. The business then can compare the reduction in exposure due to the new control to the cost of implementing the control to decide whether the control is the right investment for their company.









Network segmentation control initiative example

In this example, a company is using Axio's Control Initiatives tool to test the impact of introducing network segmentation.

For the company to test the network segmentation control initiatives, it would alter one of the key values in each cyber event scenario: the number of computers affected.

The other values will not be affected by the new control, but a segmented network will reduce the number of computers that get ransomware and the number that are affected by a network outage. Using the Control Initiatives framework, the values for all scenarios can be changed in one place, allowing the user to see how introducing the control would affect their exposure across all scenarios.

 Ransomware		 Base	 New
Variables	Number of affected computers	300	100
	Cost to replace computer	\$1000 each	
Formula for equipment replacement		300 computers * \$1000 each	100 computers * \$1000 each
Total exposure		\$300,000	\$100,000
IMPACT OF IMPLEMENTING CONTROL ON EXPOSURE: reduction of \$200,000			

 Network Outage		 Base	 New
Variables	Number of affected computers	300	100
	Cost to replace Incident response hours per computer	10	
	Incident response hourly rate	500	
Formula for equipment replacement		300 computers * 10 hours * \$500/hr	100 computers * 10 hours * \$500/hr
Total exposure		\$1,500,000	\$500,000
IMPACT OF IMPLEMENTING CONTROL ON EXPOSURE: reduction of \$1,000,000			



If the company knows that segmenting their network will cost them \$10,000, with the addition of the control initiative data points, they can now confidently invest in network segmentation, since **it will result in an estimated risk reduction of \$1,200,000.**

Axio's Control Initiatives feature provides a powerful tool for security and risk leaders to prioritize and justify investments (or divestments) in controls in the context of the business. Control changes can be easily prioritized based on their cost and how they would reduce susceptibility to or impact from a modeled cyber event.

Once a company implements a control initiative within its organization, the company can indicate in Axio360 that the control initiative is complete. They will get a log of the controls that were changed and quantified changes in exposure that resulted, which allows them to report progress to boards in financial terms.

Manage Cyber Risk on an Ongoing Basis

Ongoing management is an essential part of Axio's approach to cyber risk quantification. The cyber risk landscape changes rapidly. So do businesses. Failing to keep cyber risk data up to date leaves companies exposed.

In Axio's platform, it's easy for stakeholders to update their cyber risk information routinely or set up the platform to automatically receive data from their organization for continuous updates. By enabling businesses to own every input and easily change values at any time, Axio ensures that cyber risk management is part of the regular business planning and decision-making processes. Axio360 also makes it simple for users to continuously share progress with company leadership and the board with dynamic dashboards and generated reports.

Axio Makes Cyber Risk Quantification Accessible

Axio's methodology and process are grounded in its belief that cyber risk quantification must be transparent, efficient, and actionable—so cybersecurity leaders can quickly and easily translate their cyber risk into clear business terms.

Axio makes cyber risk quantification approachable, so clients are in control – because Axio believes clients know their businesses best.

Transparent

Axio's methodology is built on transparency. Clients own—and have access to—every input. Axio360 lets users show their work, giving them the ability to control and understand each calculation, assumption, and justification.

Efficient

Axio's method and platform enable businesses to assess and start improving their cyber risk program in a matter of hours (without an army of staff or consultants). And Axio and its partners have deep and wide-ranging experience. Their knowledge, combined with their ability to draw insights from the Axio community of users, positions them to help companies figure out where to start their cyber risk quantification process. With Axio360, businesses are in control of their cyber risk management process. The platform is easy to use and highly configurable. It is painless for companies to update their information when situations change. The platform can even be connected to certain company-internal sources of data for dynamic updating of key information.

Actionable

Axio takes a holistic view of cybersecurity by combining Cyber Program Planning and Management, Cyber Risk Quantification, and Insurance Stress Testing modules in one platform. Quick view and summary results are provided in Axio360's dynamic dashboards and generated reports. This comprehensive approach gives business leaders the ability to quickly prioritize what matters most—and act. Companies can create and manage a work plan in Axio360 to improve their cyber ROI and cost reduction.



Axio360 recommendations yield an average of \$431 of risk minimized for every \$1 of investment.

Bottom Line

Axio has re-engineered cyber risk quantification, expanding the scope of what it must encompass and ultimately shifting how companies should approach it. At the same time, by developing a fully transparent methodology, Axio has made cyber risk quantification more approachable and efficient.

Cyber risk quantification must be doable and actionable—because the cyber landscape is only becoming more costly and complex. According to the latest Accenture study on the cost of cybercrime, the average cost of cybercrime for an organization increased to \$13.0 million in 2018, up 12% from the prior year.^{iv}

That same report found “Improving cybersecurity protection can decrease the cost of cybercrime and open up new revenue opportunities.” Accenture estimated that a total of \$5.2 trillion is at risk globally over the next five years.

The Axio cyber risk quantification process is a methodical, understandable, and easily navigable way for companies to paint their risk picture so they can make wise investment decisions based on what matters most to the business.

About Axio

Mission

Axio is more than cyber risk management software. It's a new voice for organizations to communicate their cybersecurity programs with unmistakable clarity. We built Axio360 from the ground up, designed and perfected by the creators of the world's first information systems for cyber risk.

Our mission is to empower security leaders to define their maturity and exposure, make the best investment decisions, and ensure stability for any cyber scenario they may encounter.

Our experience has allowed us to cut through complexity and shine visibility on the unknown. Both business and security leaders can unite to take decisive action. Axio360 not only delivers a balance sheet for cybersecurity but facilitates a common language for readiness and rapid decision-making.

Team

We are a diverse team from both academic and technical backgrounds in data science, cybersecurity, insurance, IT, OT, and software development.

Our origins can be traced to 2013 when Axio began perfecting a methodology to provide professional risk consulting services for energy companies.

We launched Axio360 in 2018 to provide a powerful but easy tool gleaned from our knowledge, a combination of all our experience and know-how. Currently 700+ organizations trust Axio360 to protect tens of millions of end users from risk scenarios previously not defined.

Expertise

We service key critical infrastructure industries with the most complex cyber risk such as operational technology and Infrastructure. Axio360 allows:

- CFO and CISO cybersecurity language unity
- Risk understanding in dollars and cents
- Relatable risk transfer for cybersecurity strategy
- Understanding of your entire insurance portfolio (hint: there are no silver bullets)

Notes

Demo

Watch a demo of Axio360 on axio.com/view-demo

Footnotes

ⁱ [Measuring & Managing the Cyber Risks to Business Operations](#), Ponemon Institute, December 2018

ⁱⁱ [Equifax Data Breach Settlement](#), Federal Trade Commission, January 2020

ⁱⁱⁱ [The Urgency to Treat Cybersecurity as a Business Decision](#), Gartner, February 12, 2020

^{iv} [Ninth Annual Cost of Cybercrime Study](#), Accenture, March 6, 2019