
axio
Solving Cyber Risk™

In today's security landscape, cyber events aren't merely a possibility—they're inevitable. There is no silver bullet to stop motivated attackers with constantly evolving capabilities. Impenetrability is a myth. But there is a solution. Axio is accepting the challenge to bridge the cybersecurity gap.

Axio is solving cyber risk.

Redefine the Rules

Axio is creating a paradigm shift. By applying risk management strategies to cybersecurity, we've found a way to solve the unsolvable. Our approach helps firms assess the latest advances in technology, policies, and procedures and combine them with leading-edge hedging strategies.

We give you the ability to confidently and continually:

- Understand your cyber exposure
- Deploy mature defenses and mitigation capabilities
- Achieve the financial ability to recover from an event

Axio's Quadrant.
One tool. Powerful insights.

Axio moves beyond the theoretical to help you see what's at risk. Our process for solving cyber rests on a four-quadrant system of classification. It's how we clarify a cyber world that otherwise consists of an infinite number of attack scenarios and culprits, technology failings, and possibilities for human error.

Despite that endless universe, the impact of a cyber event is limited to four simple categories:

- **First party financial damage**, or financial damage within your own organization
- **First party tangible damage**, or tangible damage within your own organization
- **Third party financial damage**, or financial liability to others outside your organization
- **Third party tangible damage**, or tangible liability to others outside your organization

This taxonomy is further broken down into subcategories within each quadrant, providing specificity across the possible types of financial and tangible loss.

	First Party Damages	Third Party Damages
Financial Damages	▪ **Response costs:** forensics, notifications, credit monitoring ▪ **Legal expenses:** advice and defense ▪ **Revenue losses** from network or computer outages, including cloud ▪ Cost of **restoring lost data** ▪ **Cyber extortion** expenses ▪ Value of **stolen intellectual property**	▪ **Consequential revenue losses** ▪ **Restoration expenses** ▪ **Legal expenses** ▪ **Civil fines and penalties** ▪ **Shareholder losses**
Tangible Damages	▪ **Mechanical breakdown** of your equipment ▪ Destruction or **damage to your facilities** or other property ▪ **Environmental cleanup** of your property ▪ **Lost revenues** from physical damage to your (or dependent) equipment or facilities (business interruption) ▪ **Bodily injury** to your employees	▪ **Mechanical breakdown** of others' equipment ▪ Destruction or **damage to others' facilities** or other property ▪ **Environmental cleanup** of others' property ▪ **Bodily injury** to others

Control Your Cyber Future

Establishing a strong foundation is the key to continually tackling cyber risk. Knowing what actions to take requires understanding your potential risk, the extent of your insurance portfolio, and the maturity of your controls. Axio delivers this key knowledge through an annual three-component process—the crux of our services, which takes shape in as little as two days.

Exposure Quantification

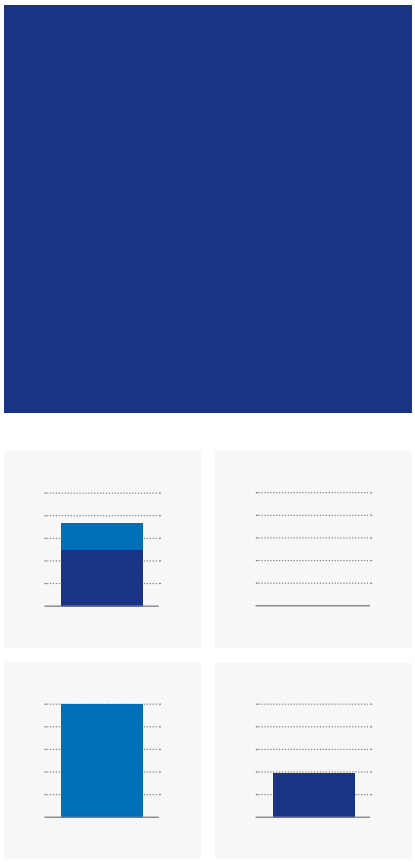
Based on firm specific cyber loss scenarios

Insurance Analysis and Stress Test

Considers the entire P&C portfolio

Cyber Program Evaluation

Utilizes C2M2, a maturity approach mapped to the NIST CSF, or other models

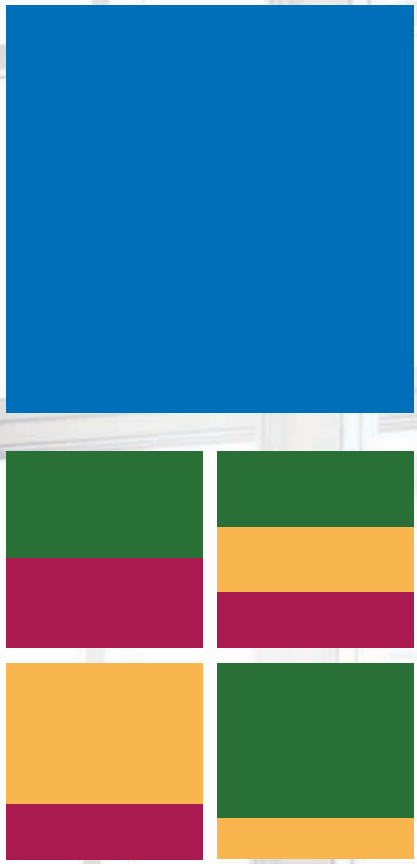


Exposure Quantification

Axio experts collaborate with key members of your team in an on-site quantification workshop. We start by generating a representative set of likely cyber loss events based around how technology is utilized throughout your organization. These are then refined to focus on the greatest potential impacts and to cover as much of the cyber risk spectrum as possible. Using a combination of external information and institutional insights, we then estimate costs, losses, and liabilities across each of the scenarios. The output is summarized in Axio's Quadrant for a clear snapshot into your exposure.

Stress Testing Output: Axio's Quadrant shows your greatest area of financial exposure, and how an event impacts your bottom line.

Insurance Coverage Balance Sheet Impact



Insurance Analysis and Stress Test

Axio's independent insurance analysis evaluates each and every policy within your property and casualty portfolio to determine how each would respond to a cyber-predicated loss. We present detailed policy-by-policy findings in the Quadrant, revealing whether each policy provides affirmative, negative, or uncertain coverage. Combined with exposure quantification, the stress test uncovers how much of the impact of each quantified scenario is recoverable through current insurance and how this will affect your balance sheet.

Axio's team can partner with your broker to clarify and enhance coverage—especially within policies where cyber has never been a factor.

Cyber Coverage Diagnostic: Resulting analysis is expressed through the Quadrant, detailing where your portfolio contains:

- Explicit Cyber Coverage
- Silent or Certain Problematic Provisions
- Strong Cyber Exclusions

Cyber Program Evaluation

The maturity of your company's cybersecurity program dictates how nimbly you can react to the ever-changing landscape of cyber risk. Using the evaluation model C2M2, Axio conducts an on-site workshop with cybersecurity leaders and personnel responsible for the performance of the model practices. We discuss each practice and participants evaluate its implementation level, resulting in a detailed C2M2 scorecard with a graphical summary.

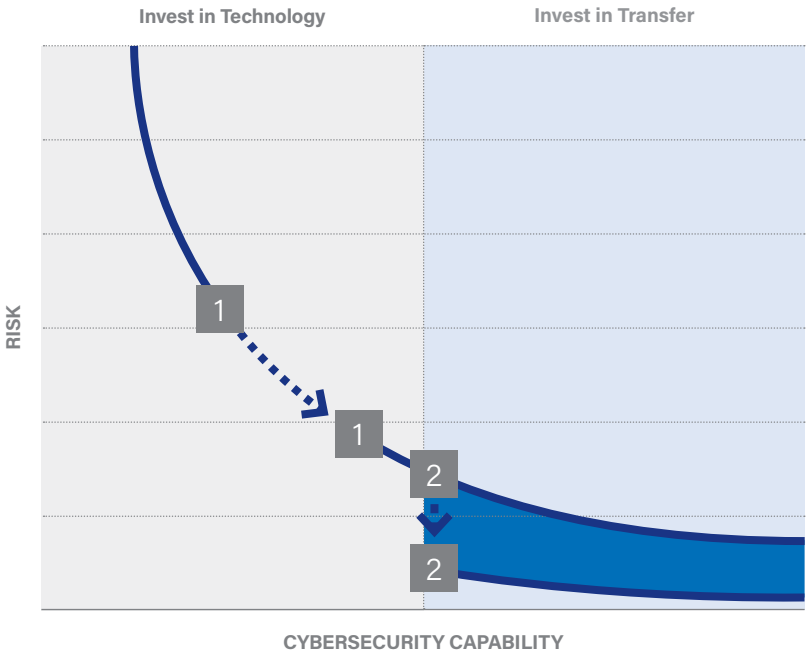
The C2M2 model consists of ten cybersecurity domains and three maturity levels. Each individual circle represents how many practices within each domain and level have been fully, largely, partially, or not implemented—leading to a cumulative maturity level within each domain. If evaluations are conducted on multiple parts of the firm, a benchmarking view can be generated.

C2M2 Results Excerpt: Graphical indication of practice implementation across ten cybersecurity domains and thirty maturity levels.

Fully Implemented Largely Implemented Partially Implemented Not Implemented

Solutions in Action

Axio's process gives you the keys to continually manage, minimize, and transfer your cyber risk. Doing so is possible through the right combination of technologies, policies, procedures, and financial controls. Our approach shows you which tools will be the most effective for your unique business and your individual risks—moving all your loss scenarios as far down the risk curve as possible.



Cyber Risk Reduction Curve
Investing in the right combination of technology and insurance provides maximum risk reduction.

1 Technology Risk Reduction
2 Insurance Risk Reduction

Customized Partnerships

Axio's core process is intended to be repeatable, allowing for ongoing understanding and management of risk. Our extended customized engagements help you develop and execute a targeted cyber program improvement plan, conduct lateral benchmarking across your enterprise or industry, and implement more complex loss scenario modeling.

Cyber Risk—Solved.

The best barometer for measuring success is how you react to a real event. Too often, firms are left wondering how an event could've happened to them or why they didn't deploy a control that seems obvious in retrospect. Axio knows impenetrability is impossible—but cyber risk management maturity is within reach. We offer a partnership to ensure you understand your exposure, manage it effectively, and are equipped to financially recover.

Cyber events won't wait for you to be ready. Contact Axio today.

axio

Axio 77 Water Street, 8th Floor, New York, NY 10005 USA info@axio.com axio.com