Axio is 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 cyber resilience is readily achievable.

Axio is creating a paradigm shift. By applying risk management strategies to cyber security, we've found a way to solve the unsolvable. Our approach helps firms assess the latest advances in technologies, policies, and procedures and combine them with leading-edge hedging strategies. The Axio process is designed to empower security leaders, senior executives and boards of directors with the ability to confidently and continuously answer the three most important questions in cyber risk management:

1. *What is my cyber exposure?*
2. *Are my cyber defense capabilities sufficiently mature?*
3. *Do I have the ability and financial resources to recover from a meaningful cyber event?*

Each question is answered by a step in the Axio360 process; each of which is described in the following sections.

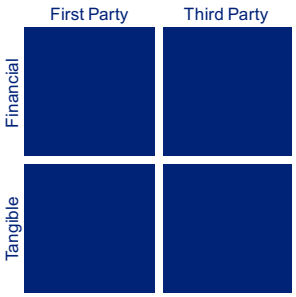
Exposure Quantification

Understanding the types and scale of impacts that could arise from a complex cyber event is a critically important step in managing cyber risk.

Exposure quantification is accomplished in a one-day workshop, which can be scheduled as one full day or in several meetings. In the workshop, Axio leads a structured discussion with cybersecurity and other subject matter experts from the client to brainstorm plausible high-impact cyber loss scenarios and develop impact estimates for a selected subset.

Scenario identification is structured to cover the spectrum of potential cyber event types and the range of business assets and operations.

Impacts for the selected scenarios are estimated based on Axio's 4-quadrant impact model: first-party financial, third-party financial, first-party tangible, and third-party tangible.



Axio's Impact Model: all cyber impacts fit these quadrants

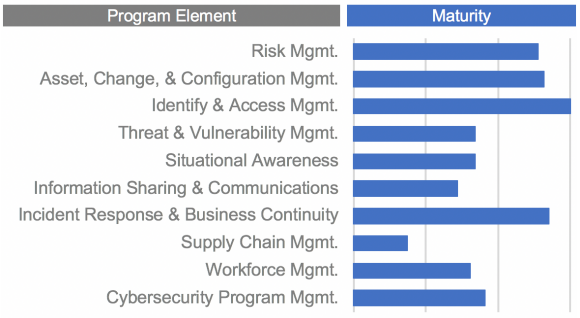
Workshop outcome includes a gross impact estimate for each of the four quadrants for each of the prioritized loss scenarios (typically 3 to 7 scenarios total).

Successful workshops typically include participants from the IT and OT cyber-security programs (as applicable), risk management, operations, finance, and legal.

Cyber Program Evaluation

The cybersecurity program is an organization's first line of defense against cyber risk. Ideally, the maturity of the cybersecurity program should be scaled to the organization's own risk profile, which becomes much more effectively accomplished after gaining an understanding through the quantification process.

Using a reference maturity model for cyber program evaluation provides a common language, consistent scoring, a roadmap for investment and improvement, and the potential for peer and internal benchmarking.



Axio supports the NIST Cybersecurity Framework (NIST-CSF) and the Cybersecurity Capability Maturity Model (C2M2), developed by the US Department of Energy, as the basis for cyber program evaluations. These models are widely adopted and cover both traditional IT security and the security of operational technology (OT or industrial control systems). Most organizations have at least some OT systems for building or power controls.

The cyber program evaluation is accomplished in a one-day workshop, which can be scheduled as one

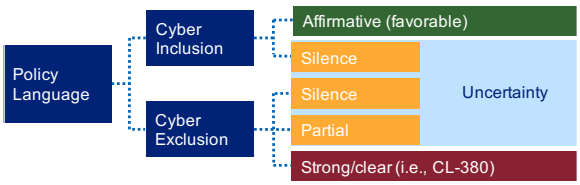
full day or over the course of several meetings. Participants from the organization's cybersecurity program are needed.

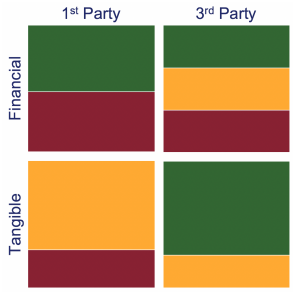
The output includes a maturity score and identified gaps for each of the sections of the model.

Insurance Analysis & Stress Test

To understand the organization's ability to recover financially from a complex and costly cyber event, we must understand how the insurance portfolio will respond.

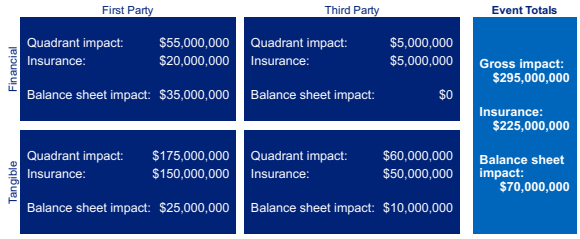
Axio first analyzes all policies in the portfolio to discover how they are worded with respect to a cyber peril. The following logic is used to evaluate the coverages.





Insurance coverages map directly to the Axio 4-quadrant impact model. The quadrants are used to summarize the analysis output. Analysis comments are provided to explain the summary.

After the analysis is complete, Axio uses the quantified loss scenarios from the Exposure Quantification process to stress test the insurance portfolio. Insurance recoveries are estimated for each of the impacts from each scenario. This provides the necessary data to determine how each of the quantified scenarios could impact the organization's balance sheet.

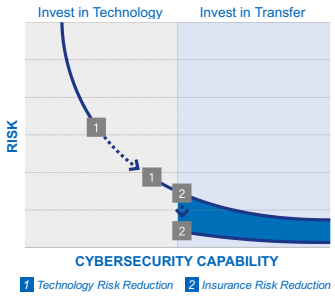


The insurance analysis and stress testing is performed offsite and briefed by phone or onsite.

Key Benefits

The proposed foundational cyber risk management process will yield the following primary benefits:

- Understanding of how a meaningful cyber event could impact your operations, finances, and assets.
- Awareness of current cybersecurity program maturity and potential improvements.
- Improved ability to manage cyber risk and protect the returns on key assets.
- Actionable insight to help optimize cyber risk investment. As shown in the diagram, for some loss scenarios, the best investment will be in cybersecurity capabilities; for others, it will be in fine-tuning the risk transfer capacity (i.e., insurance). Optimizing the mix of controls will provide the best route to achieving your desired position on the risk curve, or best protecting your balance sheet and reputation.



Cyber Resilience Platform

Partnering with Axio includes a one-year enterprise license to the Axio360 platform. The current, and intended evolution of the platform includes:

1. NIST-CSF & C2M2 Capability (Available): Allows an organization to conduct one or more evaluations, set improvement targets, track progress relative to historical posture and report on improvement progress.
2. Quantification (Fall 2018 Release): Helps an organization construct and maintain a catalog of firm specific cyber loss scenarios and scenario specific impact estimates.
3. Insurability and Stress Testing (Fall 2018 Release) Integrates the organization's insurance portfolio and cyber coverages and integrates with the quantification results to show a real time estimate of anticipated insurance recovery.
4. Benchmarking: Comparison to peers for all three components.