

Global Manufacturing Company Gets a Holistic View of Cyber Risk in Financial Terms



Manufacturing Entity Justifies Cyber Spending and Maximizes the Benefits of Their Cyber Program

Axio was approached by a global, publicly traded manufacturing company with two primary concerns:

- Their cybersecurity spending had been increasing, but the CFO was unable to get an answer as to the efficiency of that expenditure.
- The Board and management team struggled to prove that they met their duty of care with respect to managing their cybersecurity program.

Our client wasn't unsophisticated — they spent significant sums of money on preventative measures and had a robust view of the potential threat landscape — but they struggled to get a holistic view of their risk in financial terms and effectiveness of their spending on technology and insurance. Recognizing their duty to customers and shareholders, the manufacturer knew that it needed to start talking about cyber risk in dollars if they were going to justify their spending and maximize the benefits of their cyber program.

In fact, the SEC had just highlighted this approach in their updated February 2018 guidance, stating, *“the cost of ongoing cybersecurity efforts (including enhancements to existing efforts), the costs and other consequences of cybersecurity incidents, and the risks of potential cybersecurity incidents, among other matters, could inform a company’s analysis (of its financial condition).”*

Axio immediately recognized the problem and suggested a change in tactics from a compliance and controls approach to a risk-based approach with our four-part methodology. First, an Exposure Quantification was performed to create a financial picture of the manufacturing company's risk scenarios. This identified specific outcomes across the risk spectrum that could impact the company and its customers, and assigned monetary losses to each. Next, an Insurance Analysis and Stress Test was performed, mapping the discovered loss scenarios against the portfolio of insurance and financial reserves. In this case, the manufacturing company discovered a scenario centered on cyber-predicated tangible damage that fell outside the scope of their insurable losses and caused damage in excess of their tolerance.

Axio was able to point the client to an innovative insurance policy covering this type of event, allowing them to eliminate \$20 million of risk for a modest premium. Following this, Axio delivered a Program Evaluation to evaluate the maturity of the manufacturer's cyber program



“ ”

Axio was able to help us understand our risk in financial terms and quickly shed light on how effective our cyber programs was based on real data and current spending on technology and insurance.

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

and help define the optimal target state utilizing data Axio has gathered from hundreds of prior evaluations. Finally, the client was benchmarked against their peer group, and gaps to bestpractices were identified in short order.

Upon completion of the Axio process, our client's concerns were alleviated. The CFO could point to specific monetary risks that had been eliminated by the current spending and had a framework to analyze future iterations of proposed cyber defenses. The Board was able to point to a benchmarking study proving they operated a cyber program more mature than a majority of their peers, with their target state pointing to a top quartile threshold. The technologists, risk managers, C-suite executives, and Board members were able to collaboratively discuss cyber risk in a common language and begin to evolve their cyber maturity as a cohesive unit.

About Axio

Axio knows that impenetrability is impossible, but cyber resilience is within reach. We recognize that technology is only part of the solution, insurance should be treated as a critical control, and that making risk-based decisions is the most optimal way to succeed. We help organizations effectively align controls and capabilities to minimize cyber risk and maximize the ability to recover fully when security failures occur. Axio's platform and services provide all stakeholders with a common framework to proactively manage cyber risk in terms that the entire organization can understand. CISOs can continuously monitor the company's cyber posture and confidently invest in the right capabilities to reduce risk. Risk officers can optimize their insurance portfolio and structure the right coverage to protect their business. Board members and executive leadership can now be confident that their cyber strategy will achieve and sustain resiliency. Axio delivers Cyber Resilience Optimization.

Get Started with Us

If you are interested in learning more about other energy engagements with Axio, contact an Axio representative to arrange for an evaluation of your cybersecurity capabilities and resilience and learn how Axio can help your organization proactively manage cyber risk.



Learn more at www.axio.com, follow us on Twitter [@axio](https://twitter.com/axio), or email us at info@axio.com.

77 Water Street ■ 8th Floor
New York, NY10005 USA
info@axio.com