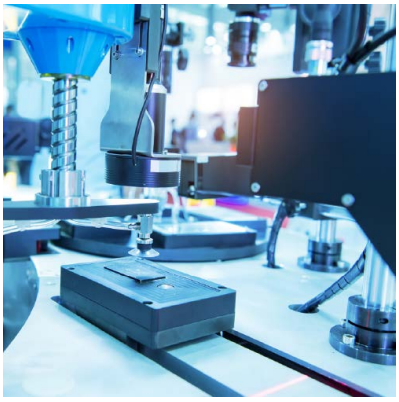
Medical Device Manufacturer Gains Confidence In Cybersecurity Spending And Program Maturity



Axio was approached by a publicly traded medical device manufacturer with two primary concerns:

- The CIO wanted to validate the effectiveness of their cybersecurity program in addressing the postmarket cybersecurity considerations of their medical devices.
- The Board and management team struggled to prove that they met their duty of care with respect to managing their cybersecurity program, including their understanding of the risk of patient harm.

Our client operates in over 30 countries and their networked medical devices are used in hundreds of procedures every day. Given the nature of the shared responsibility of securing their medical devices across all of their stakeholders, they struggled to get a holistic view of the risks posed both to and from their devices and the surrounding network infrastructures that they are deployed within. In particular, the medical device manufacturer wanted assurance that it was doing enough to mitigate the tangible impacts that a malware attack could have and the resulting risk of patient harm. Furthermore, they wanted to ensure that they had a complete picture of their risk in financial terms and the effectiveness of their spending on technology and insurance to safeguard against these types of attacks.

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 enabled by Axio360. First, an Exposure Quantification was performed to first identify the risk scenarios associated with the networked medical devices and second, to create a financial picture of those risk scenarios, including a malware attack. Axio identified specific outcomes across the risk spectrum that could impact the company and its patients and assigned monetary losses to each.
Next, an Insurance Analysis and Stress Test was performed, mapping the discovered loss scenarios against the company’s portfolio of insurance and financial reserves. In this case, the device manufacturer discovered a scenario centered on cyber-predicated tangible damage that fell outside the scope of their insured losses and caused damage in excess of their tolerance, a problem that was fixable via a modification to the insurance portfolio.

> *“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, NY10005 USA
info@axio.com

Following this, Axio delivered a Program Evaluation to evaluate the maturity of the device manufacturer's cyber program 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 in the best practices applied by the device manufacturer were identified in short order.

Upon completion of the Axio process, our client's concerns were alleviated. The CIO could point to specific cybersecurity controls and practices that demonstrated a duty of care across the device lifecycle and had a framework to analyze future iterations of proposed cyber defenses. 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. The Board was also 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, a key contributor to the newfound confidence that they were meeting an appropriate duty of care.

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.

axio®

Learn more at www.axio.com, follow us on Twitter @axio, or email us at info@axio.com.

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