Customer Success Stories

A Medical Device Manufacturer Achieves Cyber Resilience

Axio worked with a client in the medical devices manufacturing space that had 2 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.

The Problem: Ensuring Proper Cyber Controls Guard Patient Care

Our client operates in over 30 countries and their networked medical devices are used in hundreds of procedures every day. The organization 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. Following SEC guidance, 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.

Solution: Extending Your Cyber Risk Visibility with Axio360

Using Axio360, the client performed an Exposure Quantification 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.

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.

Collaborative Cyber Security Decision Making

The CIO could now 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.

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

CISO
Global Medical Device Manufacturer

Axio360 Enables:

- Dynamic risk-based decisioning
- Cyber program maturity
- Actionable results within 48 hours

Gartner COOL VENDOR 2020

Contact us to learn more: sales@axio.com