**The Great Translator: The Power of Cyber Risk Quantification Towards Cybersecurity Maturity**

**By Scott Kannry, CEO of Axio**

One of the biggest obstacles to achieving cybersecurity maturity is a language barrier: security leaders speak tech, risk managers speak insurance, the legal team speaks contracts, CFOs speak ROI, and the C-suite and Boards of Directors speak duty of care and financials. In practice that translates to business leaders not understanding how operations can be impacted by a cyber event, money being spent in the wrong places, and a lack of coordination of critical functions.

With collaboration like that, it’s no wonder that in the aftermath of most large events, the common refrain sounds something like “We never knew that such an event could happen to us; we thought our people were doing the right things; we thought we had the right controls; we thought we bought the right insurance.” In this day and age, that’s nearly a guaranteed recipe for terminations, director’s and officer’s litigation, and financial outlook downgrades from Moody’s.

Is there hope? After all, the dynamics articulated above present quite a challenge because most of the key stakeholders have different personal competencies, manage distinctly different functions, report through different silos, and exist at different levels of authority.

Luckily the answer is yes, and it’s our belief that utilizing quantification as part of an organization’s cybersecurity strategy can serve as the great translator.

Quite simply, quantification is what translates cybersecurity to the business in terms of dollars. It’s a language that all of the key stakeholders should be able to understand and collaborate around, else they shouldn’t be key stakeholders. Think about it as analogous to financial management and reporting as far as the cadre of commonly used tools—the balance sheet and income statement (P&L). Each of those tools and the combination of them all is what allows organizations to translate the performance of its good and services, everything that goes into the production of those goods and services, and everything that needs to be contended with as a byproduct of those goods and services, into a universally understood and actionable framework.

When deployed effectively, cyber risk quantification can provide that same benefit. For example:

* **Security leaders** can prioritize security investments more effectively. Imagine yourself as just having received the security assessment report from your consultant, and they’ve identified 12 critical vulnerabilities with an expensive price tag to mitigate. How can you effectively argue for more budget if your CFO is getting wary because he or she gave you everything you wanted the last three times, and the company hasn’t had a cyber event since? With cyber risk quantified, you can make the case more effectively, if for example you can show that 4 of the deficiencies could result in $500M losses, 4 of the deficiencies could result in $100M losses, and 4 of the deficiencies could result in $1M losses, therefore you’d really like funds to fix the top 4, would still like funds to fix the middle 4, and for now can pass on the minor 4. Feeling better about requesting $1.5M of the $2M remediation price tag?
* **CFOs** can adjudicate budget requests more fairly. Imagine yourself contending with a new request from the risk manager for money for a new cyber insurance policy and the security leader for a new control. What do you fund if you are nearly maxed on budget for the year? How do you compare and make the most effective decision? With cyber risk quantified, you’d be able to understand, for example, that spending $50,000 on a new insurance policy that transfers $20M of loss is a more effective investment than spending $50,000 on a control that only further minimizes the possibility of a $10M event from happening, especially if the policy would cover that event.
* **Business leaders** can manage the risk proactively and prevent it from even existing. Imagine yourself as the GM of a division and you’ve just received a proposal from a consultant to replace a series of manual failsafe controls with remotely controlled models and part ways with the two engineers that monitored the valves, thus saving $175,000 annually. No brainer! Or is it? With cyber risk quantified and the requirement that decisions like that get run through a quantification simulation, you might want to pass because as GM you’ll now own the $800M cyber event that you’ve potentially enabled.

* **Investors** can rate and report cybersecurity risks consistently. Imagine yourself as the fund manager at a private equity firm. Hopefully your portfolio companies are reporting on cybersecurity on a periodic basis, but what are they giving you? Technical performance reports? What does that indicate as far as what risk you and your investors own, even if everything looks good? With cyber risk quantified, you can understand what a cybersecurity event at a particular portfolio company can mean to the portfolio and where should you pay attention. For example, dig deeper at the company whose cybersecurity risk is $500M, not $5M.
* **Boards** can fulfill their fiduciary responsibilities. Imagine yourself at the quarterly board meeting and you just finished hearing from the CFO. The balance sheet looks strong—the company has plenty of cash and has just refinanced an unfavorable note, and increasing sales makes it appear as if you’ll beat the street’s estimate for the second quarter in a row. Now the security leader presents, and you receive a heatmap with greens, yellows, and reds, as well as 50 pages of supporting detail. How does that make you feel? Slightly uncertain? With cyber risk quantified, you’ll hear that the company is currently spending $500,000 per quarter to defend against $50M of risk, which is down from $60M two quarters ago and is projected to be at $45M at the end of the upcoming quarter. Feeling less uncertain and more like you are fulfilling your fiduciary responsibility?

There’s no doubt that when the right approach is taken, leveraging cyber risk quantification as part of an organization’s cybersecurity program can drastically improve how the potential impact is managed. The front-line leaders—security, risk, legal, human resources, and others—can play the team game that needs to be played and not battle over dollars based on individual interests. CFOs can have confidence that funds are being spent in the most effective areas. C-suite executives and Board members can understand the risk as it relates to the business and therefore drive decisioning in a way that fulfills their fiduciary responsibility.

Let’s revisit how most companies react to large cyber events but imagine the difference with cyber risk quantified. The narrative fundamentally shifts to something more mature: “We’ve experienced an event that we knew was possible and that we prepared for; because we knew where to invest, it’s far less severe than otherwise could have been possible; and because that knowledge enabled us to proactively purchase the right insurance portfolio, we’ll be able to cover the loss.” That narrative, contrary to the first, shouldn’t result in any terminations, D&O suits, or Moody’s financial outlook downgrades. That’s the power of quantification as the great translator.

At Axio we believe that every organization can solve their unique cyber risk challenges, and that cyber risk quantification is a key driver of success. To deliver on that belief, we built an intuitive and user-friendly quantification methodology and SaaS solution that helps organizations achieve all of the benefits articulated above. And unlike most mainstream methodologies that produce a complex annualized average risk value that most often vastly underestimates the potential impact of a significant event to the business, Axio’s proprietary methodology and software allow users to easily construct a portfolio of representative cyber events. Each of those events has an associated dollar impact value, broken down by financial, tangible, and liability impacts. Axio’s solution allows an organization to focus on what matters the most and make more effective decisions as to where to direct cybersecurity capabilities.

To learn more about Axio360 and how our proprietary methodology works, visit [www.axio.com](http://www.axio.com) or [request a demo here](https://www2.axio.com/signup-CRF).

**About Axio**

Axio is a leader in cyber risk management. The Axio360 platform is the only methodology and software that empowers organizations to continually answer the four most critical questions for cyber risk:

1. What’s my exposure in financial terms?

2. How should I manage my cyber program?

3. Do I have the financial ability to recover from an event?

4. Where should I invest?

Answering these four questions enables actionable visibility into cyber risk so organizations can focus on the right decisions to drive the business forward.