EXTRAHOP™

The Dangers of Cyber Risk Quantification

Reporting on cyber risk can get risky. Three current and former CISOs share their experiences.

By Michael Clark

Cyber risk quantification (CRQ) is an approach to analyzing and reporting on cybersecurity risks that has grown in popularity over the past decade. One of the leading CRQ frameworks is known as the Factor Analysis of Information Risk (FAIR) model. The FAIR model posits that cybersecurity risk can be quantified in terms of its potential financial impact, just like any other business risk. The benefits to quantifying risk financially are that security leaders can communicate the impact of a potential cybersecurity incident in terms executives are familiar with and they can clearly demonstrate the effectiveness of their cybersecurity programs.

But CRQ isn't one size fits all. In fact, quantifying cyber risk in financial terms can sometimes backfire, which, ironically, makes CRQ risky. ExtraHop sat down with three current and former CISOs to get their opinions on the merits of CRQ and how best to approach it: Sam Curry is the CISO at Zscaler and has over three decades of experience as an entrepreneur, infosec expert, and executive; Julian Cohen, former CISO at Ocrolus, began his cybersecurity career as a contractor for the Department of Defense before moving into the private sector; and Jerry Perullo is the former CISO of the New York Stock Exchange, founder of Adversarial Risk Management, and Professor of the Practice at the Georgia Tech School of Cybersecurity and Privacy.

Beware the Dangers of Quantifying in Dollars

When many people think about cyber risk quantification, they often think of quantifying in monetary terms, but both Perullo and Curry caution their peers against quantifying cyber risk in dollars for a variety of reasons.

For one, using a large dollar figure to convey your organization's cyber risk exposure is likely to cause panic or inspire deep skepticism, according to both Curry and Perullo. Either way, your credibility could take a significant hit.

"Half the directors will think that's a very high estimate and half will think it's a low estimate. But all of them will think you're wrong."

"If you go into a board meeting and say there's a $20 million risk associated with your organization being the victim of a ransomware attack, half the directors will think that's a very high estimate and half will think it's a low estimate. But all of them will think you're wrong," says Perullo. "The board's expertise is in the business, so if you make bold claims that aren't accurate, they won't take you seriously."

The other drawback to quantifying cyber risk in financial terms is that you may inadvertently prompt business leaders to make a potentially bad decision that you didn't anticipate. For example, when Curry was working for EMC after its acquisition of RSA, leaders at RSA attempted to quantify in dollars the risk of a cyberattack on its identity business. With half a billion identities under their management, they estimated that RSA's $200 million business unit carried over one hundred times the risk of the entirety of EMC's $24 billion enterprise class risk.

"The natural conclusion of EMC leadership after seeing this number was that they needed to sell off the identity business because the risk of holding on to it was way too high, despite the fact that RSA's identity business constituted 30% of EMC's net operating margin," says Curry.

Cyber Risk Quantification Challenges

While it sometimes makes sense to frame certain enterprise or operational risks in dollars, Perullo doesn't think this kind of financial modeling suits cyber. For one thing, he says, it creates potential for conflicts of interest, depending on who's doing the math and what their objective is. For another, it's hard for security leaders to accurately gauge the probability and assess the impact of cyber incidents—in part because they lack sufficient data to build those models and in part because in some ways, the probability of a cyber incident occurring is binary, according to Perullo.

"For most companies, most of the time, nothing happens. But when a cyber incident does occur, it's often a massive event," he adds.

Calculating the impact of a cyber incident is equally complex. "Given the same cyber incident, the impact could be portrayed an order of magnitude greater or lesser, depending on the story you want to tell and the cost factors you choose to take into consideration," says Perullo.

Take the example of a ransomware attack, where threat actors demand $1 million to restore systems access. The financial impact of the ransomware attack could range anywhere from $1 million on the low end to tens or hundreds of millions of dollars on the high end, depending on the size and scope of the attack (e.g., the amount and type of data compromised) and whether the individual modeling the impact factors in a wide variety of direct and indirect costs, including lost revenue, lost productivity, regulatory fines, legal fees, breach notification costs, and so on.

Alternative Methods for Quantifying Cyber Risk

If dollars aren't the most effective way to quantify cyber risk, what is? Former Ocrolus CISO Cohen says he doesn't have a preferred model or methodology. "I don't want to pigeonhole myself into a particular framework," he says. "One framework might include things my organization doesn't need to consider, while another framework may lack considerations my organization needs."

Instead of following a specific cyber risk quantification methodology or framework, Cohen prefers to begin any cyber risk modeling or quantification exercise from the adversary's perspective. In other words, he starts by asking a series of questions: What assets does my organization have that might be valuable to a threat actor? What kinds of threat actors typically target those assets? What techniques do they typically use? To what extent is my organization vulnerable to those techniques? "Once you've figured out the answers to those questions, the next step is prioritization. You might prioritize based on which assets are most valuable to threat actors, which attack methods are most common, or the estimated impact or likelihood," he says.

Perullo suggests a similar approach, but broadened to include board members, who may be aware of additional assets and risks that aren't on your radar. Once you've established the objectives of the threat actors most likely to target your organization (e.g., whether their goal is to perpetrate fraud, sabotage your operations, or steal your intellectual property), find precedents for each, and based on those precedents, create red team scenarios to test your organization's cyber risk posture and controls. Perullo emphasizes the need to be scientific about these scenarios: "There needs to be potential for the exercise to truly show whether you're investing enough, or you're biased from the start." In other words, CISOs shouldn't be designing these scenarios with an end goal (e.g., securing more funding) in mind. Instead, it should be possible for tests to show that the current program is working.

Curry advises CISOs joining new organizations to find out how the organization describes and quantifies other business risks so that they can present cyber risk in a similar manner. "Talking about risk in terms of big dollar amounts when an organization doesn't normally talk about risk that way can lead to bad decision making," he says, adding that quantifying along a scale where each increment carries meaning but isn't tied to a specific dollar amount may be a more effective approach.

Similarly, Cohen emphasizes the importance of understanding your audience and the way they prefer to take in information—albeit with some exceptions. For example, while the C-suite and board usually want metrics and to see key risk indicators improving, Cohen cautions against getting too caught up in the numbers, as they aren't always meaningful indicators of progress. "What does it really mean to respond five seconds faster to phishing emails than last quarter or to detect 80% more phishing attacks? Are these really improvements?"

All in This Together

Some of your colleagues in the C-suite are also fighting an adversary in their own way, notes Curry, who adds, “Sales, legal, and cyber all have intelligent and adaptive opponents who are actively trying to defeat them.” The CISO, obviously, faces nation-state threat actors and cybercriminals. The General Counsel fights off class action services. The CEO and Chief Revenue Officer go face to face with competitors. This is a unifying factor for many in the C-suite and can help CISOs get closer to their peers, especially the CFO and General Counsel.

Most CISOs recognize the importance of the CFO in both budget and risk management decisions, and CISOs’ relationships with their CFOs will grow in importance as CISOs of publicly traded companies get more involved in their organization’s cyber-related SEC filings. Fostering a close, peer-to-peer relationship with General Counsel is mutually beneficial, says Curry, not to mention they can provide attorney-client privilege during sensitive risk discussions.

All of this is to say that cyber risk quantification and management of cyber risks is a team sport. And while there are many ways to quantify cyber risks, from dollars to downtime, what’s important is that the method you choose clearly communicates risk, how you’re compensating for it, and aligns with the methods the rest of your management team uses. </>

Michael Clark is a marketing content writer at ExtraHop. He previously worked for Optiv Security, where he developed a wide range of assets on ransomware, operational technology, threat intelligence, and more during his nearly four-year tenure with the reseller. Outside of work, Michael enjoys bouldering and writing sci-fi short stories.