CYE

How Cyber Risk Quantification Drives Business Decisions

Introduction

In the fast-paced realm of cybersecurity, organizations must proactively address the growing menace of cyber risks. As attacks have increased, both cybersecurity budgets and board-level scrutiny on cybersecurity as a business risk have followed suit. Cyber risk quantification (CRQ) addresses these issues by calculating an organization's risk exposure in monetary terms and applying that information to make decisions about managing risk in a business context.

A compelling business case for a cyber risk quantification solution not only secures internal buy-in but also paves the way for effective risk management. The following are five benefits of CRQ that can help support your business case.

1. Better Understanding of Cyber Risk

Faced with rising threats, an ongoing shortage of cybersecurity professionals, and increased attention on the business impact of cyberattacks, CISOs must prioritize the various risks facing their organizations. Cyber risk quantification models and tools help them understand what threats exist as well as what data and business assets are at risk.

2. Cyber Risk in Monetary Terms

Once you know which business and data assets are at risk, you need to understand whether they present any real risk at all. All risks are not created equal. Part of the quantification process is understanding each probable threat and figuring out the likelihood of occurrence. What costs, including regulatory penalties, might your organization incur in a data breach? For example, GDPR fines can amount to €20 million or 4% of global annual turnover—whichever is higher. What are your most critical or expensive assets, and which ones are at highest risk?

Putting that cyber risk into concrete monetary terms can help you calculate the value of your assets in real business terms and prioritize mitigation based on both the cost of a breach and the cost to reduce threats. That information also helps you decide how much to spend on security tools and where those tools will have the greatest impact in financial terms. The identification of threats and assets is an ongoing process, not something that you can do once and move on. The evolving nature of risk and your changing environment means that you need to focus on relative risks and how to mitigate them.

3. Prioritized Risk Mitigation

Adding the financial context for identified risks is essential if you want your security team to prioritize which gaps to address first. If a threat materialized as an attack, what would be the potential damage to the business? A few examples of the potential damages and cost to the business include:

- What is the cost of shutting down a shopping website or an assembly line for a few hours, days, or more?
- What if employees are idle due to a network outage?
- Is there an additional cost to perform tasks manually instead of digitally in case of an outage?
- Are there any third-party costs, such as legal fees or costs associated with data breach reporting?

Costs are not limited to the possible cost of the cyber incident itself but also to the cost of remediation – and some of those costs relate to loss of reputation and trust by your customers and partners. Once you understand the potential business impact, how exploitable the threat is, and what it will cost to mitigate the risk, you have the information you need to decide which risks are the most critical for you to mitigate.

4. Optimized Cybersecurity Investments

You can make better budget decisions based on the real dollars at risk in the event of a breach to your critical assets. According to Gartner, by 2026, organizations are expected to spend $262 billion on information security and risk management products and services. While funding may be growing, there are many attack vectors and scores of security tools and services available, so choosing how to spend cybersecurity dollars can be difficult without the context supplied by a robust cyber risk quantification model or tool.

CRQ helps you focus on making effective decisions based on the business impact vs remediation costs. For example, when you build your budget plan for the management approval backed by real numbers rather than expected threats, it will get you the budget approval you need to build an effective security plan

5. Communication with Executive Team and Boards

A monumental shift is underway in the world of cybersecurity. This pivotal juncture marks a turning point that we've been heading towards for years. With various factors converging, from the White House's cutting-edge cyber strategy to the dynamic initiatives of organizations like CISA and the new cyber regulations introduced by SEC, including the NIST CSF 2.0, the message is clear: cybersecurity risks have become a concern that demands comprehensive organizational attention, extending beyond the CISO's domain.

It's about management addressing cyber threats as part of the broader spectrum of risks facing the organization. The imperative now is for companies to ensure persistent handling of cyber risks, encompassing systematic written assessments and the cultivation of adept organization-wide coping mechanisms.

Adopting the right cyber risk quantification model can help you ensure that decision makers fully understand the potential financial and business ramifications of different cyberattack scenarios and approve budget to implement cybersecurity solutions effectively and efficiently.

Cyber Risk Quantification Drives Business Decisions

Ultimately, CRQ is good for business. Understanding the full implications of attacks and costs can help your security team focus efforts and budgets where they will make the biggest impact and transform security into a business enabler instead of a blocker. Cyber risk quantification can help you effectively reduce cyber risk, backed by an executive team whose members understand that cybersecurity spending, done right, is an investment in the business as a whole.

Want to learn more about CYE's optimized cyber risk quantification?

Contact us

About CYE

CYE's optimized cyber risk quantification platform and expert guidance transform the way organizations manage cybersecurity. Using AI, machine learning, and innovative technology, CYE visualizes attack routes, quantifies, mitigates, and communicates cyber risk, and matures organizational cybersecurity posture. In doing so, CYE provides clear and relevant insights that empower companies to make effective cybersecurity decisions. The company serves organizations in multiple industries globally. Founded in 2012, with headquarters in Israel and operations around the world, CYE is funded by EQT Private Equity and 83North. Visit us at cyesec.com.