ThreatConnect. now a part of Dataminr.

IBM Consulting

Operationalizing Risk Quantification for Smarter Security

Cary Wise, Director, Risk Market Development

Randy Spusta, Principal, IBM Cyber Threat Management

In this joint whitepaper from IBM and ThreatConnect, learn how leading organizations are quantifying cyber risk in financial terms to make better decisions at all levels of their security organization. We'll highlight significant financial and operational benefits of adopting a cyber risk quantification approach and explore top 5 use cases that enterprises are adopting.

Table of Contents

3 Introduction

4 Cyber Risk Reporting to Executives

5 Security Spend Optimization

6 Cyber Program Roadmap Planning

7 Vulnerability Management

8 Enterprise Risk Program Development

9 Getting Started with Cyber Risk Qualification

Introduction

Leading organizations are taking cyber risk quantification from the academic to the operational to make more informed risk and investment decisions.

Organizations constantly face new tactics from cybercriminals who aim to target and compromise their most valuable assets. Yet, despite evolving techniques, many security leaders still rely on subjective terms such as low, medium, and high or green, yellow, and red to communicate and manage cyber risk. These vague terms do not convey the necessary detail or insight to produce actionable outcomes that accurately identify, measure, manage, and communicate cyber risks, leaving executives and board members uninformed and ill-prepared to manage the organization effectively.

At the same time, executives are feeling increasing pressure to improve cybersecurity programs, especially considering newly adopted regulations, like those from the U.S. Securities and Exchange Commission (SEC), requiring publicly traded companies to disclose cyberattacks within four business days and annually disclose material information about their cybersecurity risk management, strategy, and governance. Cyber Risk Quantification (CRQ) has emerged as the most effective way to maximize cyber risk management programs by translating cyber risk into specific financial impacts. [1] According to Forrester Research, "CRQ will fundamentally revolutionize the way that security leaders engage with boards and executives to discuss cybersecurity" [2]

This paper will examine five use cases and explore the benefits organizations can achieve by operationalizing CRQ.

1. SEC: Washington D.C., July 26, 2023 —"The Securities and Exchange Commission today adopted rules requiring registrants to disclose material cybersecurity incidents they experience and to disclose on an annual basis material information regarding their cybersecurity risk management, strategy, and governance."

2. Mckay, Page. January 31, 2022. "The cyber risk quantification market: When CISOs need decisions, not more dashboards."

01. Cyber Risk Reporting to Executives and Boards of Directors

News headlines of cyber attacks and zero-day vulnerability exploits have become typical conversation topics in board rooms, causing cyber risk to be one of the top 5 risks facing organizations. In today's world, it is essential for security leaders to communicate cyber risks to their boards in a clear, concise, and understandable way. Often, cybersecurity reports are either filled with too many technical details and fail to provide executives with the guidance they need to make well-informed decisions, or the reports are not clear enough, making it difficult to assess the cybersecurity risk landscape and compare it to other organizational risks. This can lead to confusion and subjective decision-making.

"News headlines of cyber attacks and zero-day vulnerability exploits have become typical conversation topics in board rooms, causing cyber risk to be one of **the top 5 risks facing organizations.**"

To improve communication with board members and executives, it is helpful for security leaders to align their cybersecurity strategy with the business's needs. By operationalizing Cyber Risk Quantification (CRQ), security leaders can provide executive-level reporting that communicates the financial impacts of cyber attacks targeting vital business assets, leading to disruptions in operations, system outages, reduced production, and costs associated with recovery. By translating cybersecurity risks and investment returns into dollar terms, boardroom conversations become less about technical nuance and more about true risk-based strategy.

Security leaders can leverage CRQ to measure their current financial cyber risk exposure across the organization and demonstrate how their investments in people, technology, and the process can improve the organization's risk profile. Additionally, they can now outline how additional funds will be utilized to minimize the financial impact of cyber risk further. This type of information allows executives to compare cyber risk financially to other organizational risks, making it easier to understand the business context of cyber risk and influencing the prioritization of investments to protect the organization against current and emerging threats.

Put simply, cyber risk is business risk and should be communicated in business terms. Using the outputs of a CRQ program, leaders can drive alignment with their boards and executive teams and improve their overall risk reduction strategies and investments.

02. Security Spend Optimization

Security executives are pressured to increase protection measures and reduce risk most cost-effectively, considering economic constraints and limited budgets. However, traditional decisionmaking methods often rely on subjective information, making it challenging to objectively justify previous or upcoming

When leaders want to maximize the impact of budget, they often evaluate the costs associated with security initiatives, such as acquiring, implementing, operating, and maintaining the initiative, but fail to assess the financial risk reduction the initiative would have on the organization. Without first quantifying the risks in the context of the current security control posture as a baseline, organizations cannot accurately quantify the effectiveness of their security initiatives or determine their next best investment. Understanding the organization's financial risk exposure allows security leaders to hone in on areas with the most significant risk reduction opportunities and prioritize security initiatives that align with the business to better mitigate the most significant risks facing the business.

By operationalizing CRQ, leaders can make strategic budget decisions using objective data to evaluate, compare, and prioritize security initiatives using financial risk reduction and ROI. For example, a large initiative might substantially reduce risk but comes with significant costs. On the other hand, a smaller initiative may not reduce risk as much but could have a higher ROI due to its lower cost. Does that mean you should do one of the other? Not necessarily, but without the real numbers in front of you, it's hard to make the right calls. Effective CRQ programs provide objective insights into the security initiative decision process in the context of organizational risks, business context, and current security controls. implemented to help make wellinformed decisions.

To optimize the effectiveness and investment in security programs, it is key to avoid investments in security initiatives that don't provide significant ROI or risk reduction. CRQ enables this process with objective data. CRQ is a valuable tool for measuring the reduction in risk associated with control improvements and the increase in financial risk exposure when controls are removed or degraded due to shrinking budgets. This allows data-based decision-making to maximize the best use of available budgets and guide cuts to the least risky investments. This helps organizations optimize security spending without compromising their risk tolerance thresholds.

03. Cyber Program Roadmap Planning

As organizations advance their digital transformation programs, aligning their security initiatives with constantly evolving threats and business needs becomes crucial. Organizations can enhance their security roadmaps by understanding the threats to the organization in relation to current and proposed security controls. Operationalizing Cyber Risk Quantification (CRQ) provides automated recommendations for control improvements prioritized by financial risk reduction.

It can be challenging for security leaders to create a multi-functional or multi-phase roadmap for their cybersecurity program while balancing the benefits of new technologies with the possible impact on their organizational cyber risk profile. CRQ offers a ruler that security leaders can use to measure the effectiveness of their cybersecurity program and predict changes in cyber risk associated with roadmap initiatives.

The first step is to quantify the financial risk exposure across the entire organization by assessing the current state of controls in relation to the most critical business assets.

This provides leadership with a clear baseline understanding of the current cyber risk level and recommendations on where to focus improvement efforts based on the financial risk reduction. Leaders can compare and prioritize these recommendations with the security initiatives on their roadmap and determine if adjustments should be made. This process can also reveal areas that may have been overlooked and offer opportunities for additional "low-hanging fruit" improvements.

This approach allows decision-makers to prioritize security initiatives based on their business needs and determine the order in which they should be implemented, ensuring the most efficient cyber risk reduction across the entire organization. By utilizing CRQ, organizations can develop a risk-based strategic roadmap for security and prioritize resource and investment initiatives according to financial exposure. These roadmaps enabled by CRQ provide the necessary business justification to showcase the importance of cybersecurity in safeguarding organizations' critical assets.

Case study

Fortune 100 Global Manufacturer

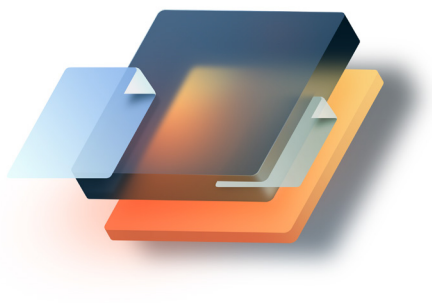
Recently, CRQ was used by a Fortune 100 global manufacturer to justify and prioritize their strategic security transformation roadmap. The organization first conducted a security assessment and identified additional initiatives that would reduce cyber risk to the organization, which were incorporated into the overall project. Since multiple initiatives were planned over the next five years, security leaders needed an objective way to prioritize which initiatives should be implemented first.

To achieve this, security leaders utilized CRQ to quantify the risk exposure given the current state of security. They then measured the effectiveness of each initiative in reducing risk to the organization. This allowed them to prioritize their strategic security transformation roadmap and prioritize implementation initiatives to drive down the most significant amount of risk first. Additionally, using ROI helped them identify "low-hanging fruit" that could be planned around the more prominent initiatives. As a result, security leaders could provide a more objective business case to justify the security transformation investment to executives and board members.

04. Vulnerability Management

Managing vulnerabilities is challenging in the rapidly changing cyber threat landscape. Traditional methods for prioritizing vulnerability remediation rely on proxies for risk, such as Common Vulnerability and Exposures (CVE) scores or the number of exposed systems, rather than actual financial risk.

Cybersecurity leaders face a continually expanding and overwhelming scope of newly identified and emerging vulnerabilities, adding to an extensive backlog of CVEs that need remediation. CVSS scoring has been the primary system used to prioritize CVE remediation efforts. While common, CVSS scores are generic and don't convey the risk a CVE introduces to the organization nor contextualize the CVE with compensating controls that would reduce risk to the organization. This leads to an environment where CVEs with a low CVSS score could pose a higher risk to the organization than those scored higher yet remain in the growing backlog of unpatched vulnerabilities.



Additionally, CRQ is utilized to assess the efficacy of compensatory measures on corporate assets when direct patching of CVEs is not feasible, either due to outdated technology or newly discovered zero-day vulnerabilities. As a tool for decisionmaking, CRQ empowers security executives to evaluate and balance the financial risks posed by the vulnerability and the expenses associated with corrective actions, such as implementing compensatory measures or upgrading the system with more secure technologies. This capability offers security executives the data necessary to make defensible judgments.

An effective vulnerability management program would not be complete without reporting and monitoring. Typical programs are riddled with inaccuracies and overwhelming details that are complex, hard to understand, and don't drive actionable results. With CRQ, security leaders can actively monitor vulnerabilities and their impact on the organization's financial risk profile. They can also generate executive-level reports demonstrating the program's effectiveness in language the business can understand. The CRQ vulnerability management program lists top CVEs, prioritized by their financial impact on the organization. This list also includes the cost of remediation and the resulting reduction in financial risk. An ROI for vulnerability management can be calculated and used to justify investments.

05. Enterprise Risk Program Development

How CRQ Fits into an Overall Organization

To provide decision makers with an overall organizational risk profile, cyber risk must be fully integrated into the overall enterprise risk management (ERM) program. But this is only possible by understanding the financial implications of cyber threats so that organizations can align their risk mitigation efforts with business objectives and enhance overall organizational resilience.

Combining technology with expertise to operationalize risk quantification is integral to an organization's Risk Management Program. This integration facilitates better decision-making across the enterprise and enables effective risk-reduction strategies. By understanding the financial implications of cyber threats, organizations can align their risk mitigation efforts with business objectives and enhance overall resilience.

Historically, many organizations have developed independent risk management procedures and processes within functional risk organizations, including Enterprise Risk Management, Cyber Security, Operational Risk, and IT Risk. Cyber Risk Quantification (CRQ) is becoming a best practice among leading organizations to develop and operate effective risk management programs, re-vamp risk scoring, and integrate enterprise risk management procedures.

Leading organizations that have leveraged CRQ to improve their management processes have developed a single, integrated operating model for risk management. They then use CRQ as the basis for identifying and managing top enterprise risks.

While this requires a fresh approach to thinking about risk management, incorporating several risk management functions, the result is a standardized, consistent, and well-understood risk identification, analysis, and reporting process. CRQ provides the foundational capability to calculate and report on cyber risk. Its adoption provides the organization with a singular definition of risk and removes any uncertainty about how to report risks to leadership and the Board. By reporting risks in terms of business impact and financial exposure, we remove the subjective interpretations that rely on nominal scales or color codes.

Additionally, having a single risk management process allows for better analytics, identifying and tracking trends across lines of business or functional areas, and systemic risks to the organization. Although it may seem daunting, organizations can take simple steps to progress on this journey.

Some of these steps include:

- agreeing on and adopting a standard definition of risk and risk categories
- ensuring that all top-reported risks identify both the business impact and financial exposure
- establishing a standard risk reporting dashboard for executive use
- utilizing CRQ to drive risk identification, evaluation, and reduction analysis

As one Chief Risk Officer recently shared,

"We noted that many risks stemming from different lines of business are similar in nature and share common root causes. Using a singular risk management evaluation process allows us to identify expected impacts quickly and, more importantly, leverage proven mitigation approaches to address those risks."

As companies continue to mature their cyber risk capabilities by adopting CRQ, we recommend that they consider incorporating CRQ into other risk functions and work towards adopting an integrated risk management operating model.

Getting Started with Cyber Risk Quantification

Whether you are trying to stay ahead of regulations, reacting to a cyber event, or being proactive, operationalizing cyber risk quantification can help your organization improve cybersecurity reporting, optimize budgets, create risk-based security roadmaps, financially prioritize vulnerabilities, and enhance enterprise risk management. By doing so, security leaders enable their executives and board members to make well-informed, risk-based, financially-responsible decisions. We recommend starting small, picking one or two use cases that best align with your organization's security goals, and integrating CRQ into business processes that drive actionable results.

> "We recommend starting small, picking one or two use cases that best align with your organization's security goals, and integrating CRQ into business processes that drive actionable results.

If you would like to learn more, feel free to contact ThreatConnect or IBM, and we can assist you in operationalizing cyber risk quantification for your organization.

Contact Info:

Cary Wise: cwise@threatconnect.com

Randy Spusta: rgspusta@us.ibm.com