Drive Business Action With Cyber Risk Quantification

Peer & Practitioner Research Published 21 March 2022 - ID G00760469 - 12 min read

By Analyst(s): Cybersecurity Research Team

Initiatives: Cybersecurity and IT Risk

Security and risk management leaders are increasingly investing in cyber risk quantification for enterprise decision support. However, only 36% report concrete results. This research will help SRM leaders use CRQ to drive risk ownership and positively affect their business decisions.

Overview

Business leaders, senior executives and board members are increasingly concerned with issues related to security and risk management (SRM). To address the worries of this ever-growing universe of stakeholders, SRM leaders, such as chief information security officers (CISOs), must provide them with meaningful guidance. Cyber risk quantification (CRQ) offers a way to communicate SRM and related implications to these stakeholders and, more importantly, drive action.

CRQ is any risk assessment that measures risk exposure and expresses it in financial or business-relevant units. The spectrum of quantification ranges from ordinal scale expressions of probability and impact to advanced statistical modeling of annual loss expectancy or the use of advanced analytics. Although the vast majority of SRM leaders have deployed ordinal scales and numerical estimates of likelihood and impact (88% and 55%, respectively), Gartner’s 2021 Cyber Risk Quantification Survey shows an appetite for increased precision. Nearly 70% of SRM leaders are planning to deploy CRQ, based on statistical modeling and machine learning (ML) techniques during the next two years.

This study identifies top challenges faced by those on the CRQ journey and best practices for driving business action at scale.
Key Findings

- Sixty-eight percent of SRM leaders aspire to use statistical modeling or ML to perform CRQ during the next two years.
- However, SRM leaders are failing to achieve substantial action-based results (e.g., risk remediation, decision influence), despite heavy investments in CRQ approaches.
- An approach that is based on a trusted analysis, timely delivery and empowering guidance to decision makers is the most effective method for quantifying cyber risk.

Recommendations

To drive business action with CRQ results, SRM leaders should:

- Reexamine conventional ways of collecting data for CRQ to maximize the use of existing, objective enterprise data that is already trusted by decision makers.
- Drive timely risk remediation by providing asset owners with different decision choices (e.g., fix critical vulnerability, run scan, set up automatic software deployment) and a clear indication of how much risk is reduced.
- Determine the necessity for scenario-based CRQ analysis by ruthlessly evaluating its impact on business decisions.

Introduction

SRM leaders try to quantify risk in many different ways (e.g., from ordinal scales, expressions of probability and impact to advanced statistical modeling of annual loss expectancy) to drive greater risk ownership and informed decision making. Our research has found a host of reasons why cybersecurity functions feel pressure to pursue CRQ, including:

- SRM leaders are unable to match business expectations with their subjective expertise, because there are too many assets, threats and demands on their time. As their organizations reach higher controls maturity and fix glaring gaps, it is harder for them to determine the ROI and the opportunity cost of varying investments — e.g., encryption, network segmentation, data loss prevention (DLP) — without methodical risk quantification.
Data-driven decision making and defensibility is becoming top of mind for decision makers. The trend for large enterprises to create cybersecurity committees with technical expertise at the board level means that SRM leaders want their risk analysis and security investments to be as defensible as possible. They believe that the rigor and objectivity of a standardized quantification approach will help them put their best foot forward.

SRM leaders are increasingly being asked to express cyber risks in monetary terms to enable comparisons with risks across the enterprise (e.g., operational, financial and health or safety risks). CRQ supports greater comparability with these other risks.

SRM leaders are tasked to support distributed risk ownership and decision making across the enterprise. This includes helping business technologists (see Cyber Judgment Presents a New Approach to Informed Risk Decision Making) manage trade-offs between multiple risks (cyber, operational, health, safety, etc.) and business opportunities. Providing quantification of cyber risks enables decision makers to better understand the cyber context and make more informed trade-offs.

Although CRQ has a tremendous potential as an approach to communicate cyber risk and drive risk-informed decision making throughout an organization, investments have not reliably borne fruit.

When asked, “What have you achieved by leveraging CRQ?” 62% of CRQ adopters report awareness-based results, such as increased credibility with nonsecurity audiences. However, only 36% of respondents answered that they have seen action-based results, such as convincing risk owners to remediate specific risks.

There are three primary reasons why only 36% of CRQ adopters achieve action-based results:

- By far, the top challenge for 52% of CRQ adopters is lack of appropriate data, especially around probability. Cyber scenario-based CRQ requires subjective probability estimates that hinge on historical data, including rare events. Even if subject matter experts (SMEs) can calibrate probability estimates using industry data, decision makers often remain skeptical of these subjective estimates.

- To compensate, SRM leaders often spend too much time running heavy analyses, failing to appreciate the importance of just-in-time communication of CRQ results in driving business action.
In addition, 46% of CRQ adopters cite tying risk analyses to specific business decisions as a top implementation challenge. Most SRM leaders take an inside-out, two-step approach to CRQ. They think about the qualitative data they can quantify (e.g., “highs” from qualitative risk assessments, their risk register) and then attempt to socialize their CRQ results with business partners. This “If we build it, they will come” mentality means SRM leaders aren’t starting with specific business decisions to guide their CRQ initiatives.

To address these three challenges, Gartner research found that those SRM leaders who consistently drive action from their CRQ efforts focus on three essential elements (see Figure 1):

1. **Trusted Analysis** — Data and assumptions are transparent, defensible and business-relevant.

2. **Timely Delivery** — Risk analysis is delivered at the speed of the business need.

3. **Empowering Guidance** — Analysis preserves decision makers’ risk ownership, while illuminating decisions as easy or difficult, complex or trade-off, or other comparisons.
Build Decision Maker Trust by Reexamining Conventional Ways of Collecting Data for CRQ

SRM leaders strive for defensible data that their decision makers trust. Many SRM leaders look to address this through improved data gathering, using calibration training to improve confidence in estimates, and meticulous risk scenario selection. However, progressive leaders understand that these approaches do not ultimately improve decision maker trust. They realize that subjective estimates are still, more or less, a guess, making quantification contentious.

Progressive organizations maximize the data they can easily acquire to build objective CRQ analyses. They use a combination of external industry data (e.g., competitors’ websites, 10-K annual report with SEC, Verizon Data Breach Investigations Report) and internal data — e.g., own and peer historical incident data, SME calibrations of relevant probabilities of controls failing or threat materializing — for probability and loss magnitude estimates.
However, the most progressive organizations realize there is a shortcut in getting credible data — using what the enterprise already trusts (e.g., business impact analysis, data about hardware and software assets, vulnerabilities, criticality to operations or sensitivity of the data assets contain). By having conversations about this data, the cybersecurity function achieves a better grasp of business priorities and builds decision makers’ understanding of what data goes into CRQ analysis, while increasing their trust in cybersecurity's CRQ expertise.

CASE IN POINT

Verizon focuses on an asset-based CRQ, instead of a scenario-based approach. The enterprise’s inventory is finite, and the data is more trustworthy as it derives from agreed-on sources, such as existing business impact analysis (BIAs), business continuity plans (BCPs) and monitoring capabilities, thus making CRQ manageable at scale. It leverages trusted data sources in concert with existing risk-monitoring capabilities to create an asset-specific risk score.

More than 5,000 assets are assigned:

- A base risk score reflects the asset’s value (e.g., revenue generation, treasury value, and/or operational support of the asset) and exposure to business disruption, whether from threat actors or regulators from its architectural features (e.g., an application’s APIs or internet-facing status)

- An actionable risk score reflects whether an asset owner is within risk appetite and specific remediation options (e.g., fix critical vulnerability, run vulnerability scan) to stay within risk tolerance.

The base risk score captures the inherent risk of an asset by virtue of its environment. These assets are stack-ranked by their base risk score into different tiers (Tier 1 through Tier 10). The higher the tier, the more important an asset is to the asset owner. By stack ranking assets, while using objective data, Verizon avoids chasing data for an infinite number of scenarios.
Drive Timely Business Decisions by Reducing Decision-Making Efforts

Some progressive companies target sophisticated, “heavyweight” CRQ for specific decisions and rely on qualitative assessments for the rest. They only use statistics-based CRQ for decision support requests that come with a well-articulated business goal — e.g., whether to enter a new market, which security controls have greatest ROI, how to inform company's negotiation and risk management strategy for upcoming mergers and acquisitions (M&A) — which requires increased precision and cannot be addressed with any other tool. According to one senior risk manager, prescreening business questions before conducting the analysis can help identify where alternative, cheaper and faster means will be sufficient to drive action.

When the decision-making time frame for a requested analysis is too tight, SRM staff meet with decision makers to establish a reasonable time frame and make CRQ analysis precision trade-offs, if needed. By having these conversations in advance, SRM staff not only save effort and resources, but illuminate to decision makers how CRQ is connected to the business goals they are trying to achieve.

Instead of aiming for data perfection, some organizations use data from older CRQ analyses to become faster at conducting future ones. For example, they reuse older information collected about risk of outages due to ransomware for a risk analysis to determine the risks associated with severe weather events. They create a data library similar to the one below to calculate loss magnitude and probability from SME data sources. The data is often refreshed annually or whenever there's a significant change in the threat landscape or the controls environment, or when the company's revenue grows significantly (see Table 1).
Finally, some companies reduce the effort it takes to make a decision by simplifying their CRQ processes and building analytics on consistently available existing enterprise data. This means they can automate data collection and analysis, enabling them to deliver CRQ outputs in real time when a risk owner needs to make a decision.

### Table 1: Sample CRQ Data Reuse Library

(Enlarged table in Appendix)

<table>
<thead>
<tr>
<th>Data Category</th>
<th>Data Point(s)</th>
<th>Subject Matter Expert(s)</th>
<th>External Sources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Probability</td>
<td>Loss event probability (forecast estimate based on historical incident data)</td>
<td>Incident responders, Security architects, Security control owner</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Historical incidents</td>
<td>Incident responders, Security architects</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Peer historical incidents (e.g., competitors with similar tech stack or geographic footprint)</td>
<td></td>
<td>Competitors’ websites, 10-K annual report with SEC, Verizon Data Breach Investigations Report, Cyentia IRIS 20/20, Identity Theft Resource Center</td>
</tr>
<tr>
<td>Loss Magnitude</td>
<td>Lost revenue/lost customers from asset compromise</td>
<td>Product/Business owner</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Incident response costs</td>
<td>Incident responders – forensic, audit, Information security team</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Fines and judgments</td>
<td>Legal, Compliance</td>
<td>10-K annual report with SEC</td>
</tr>
</tbody>
</table>

Source: HighOrchid® Case Study
Verizon’s CRQ approach has automated its assessment, which consumes data that is readily available internally (e.g., results of a scan, endpoint software deployment) to produce assessments for decision makers every quarter hour. The cybersecurity team uses an in-house-built algorithm that enables it to process 2.2 billion data pieces every 24 hours to produce more than 4,000 assessments. The biggest investment in the process consists of calibrating the weight of the data that go into asset score calculations (done in partnership with SMEs and decision makers themselves). Thanks to this automation effort, an asset owner doesn’t have to wait for a monthly report from cybersecurity, but can self-serve a risk assessment by viewing an asset’s risk score via dashboard in real time.

Empower Decision Makers by Ensuring That Each CRQ Effort Is Tied to a Clear Business Decision

Most, if not all of the time, the decision maker requiring CRQ resides outside the cybersecurity function. SRM leaders must find a way to deliver CRQ outputs that are easily understood and are relevant to the decision at hand, while preserving the risk ownership of the decision maker. It has to be clear to the decision maker not only what cybersecurity recommends with CRQ analysis and why, but also how to go about implementing it.

What successful organizations have effectively done is show asset owners the world of cyber risk using analogies they understand. For example, the risk score can be shown as debt, and the action items are the currency with which asset owners can choose to pay down their debt (see Figure 2). If the risk owner’s risk score is above two points over their risk tolerance, and if they address critical findings from a vulnerability scan, they can drive the asset’s risk back down to within tolerance. Such an approach also brings optionality with actions for the decision maker — they have a menu of actions to choose from.

This encourages continuous action to drive down portfolio risk, because once an asset owner sees the connection between their action and their risk score going down, they would continuously make risk-informed decisions about their assets, because there is always debt for the asset owner to drive down.
Another approach to providing empowering guidance to decision makers is to proactively investigate the impact that CRQ has on business decision making by requesting feedback from key stakeholders. A CRQ analysis postmortem helps to assess whether CRQ was used appropriately, and if it should be used in similar scenarios in the future (see Figure 3).
Figure 3: HighOrchid*’s Post-CRQ Assessment

**Conclusion**

SRM leaders are relying on an increasingly quantitative portfolio of tools and templates to drive impact on business decisions. Leaders who intend to consistently drive action from their CRQ efforts must focus on three essential elements: trusted analysis; timely delivery of analysis; and guidance that empowers decision makers. The following recommendations can support an actionable CRQ approach:

- Leverage data already vetted by the enterprise to proxy asset values and exposure to risk.
- Drive timely business action by providing asset owners with different decision choices and a clear indication of how much risk they drive down.
Use high-powered, scenario-based CRQ only when there is a clear business decision requiring increased precision that only it can provide.

**Recommended by the Authors**

Infographic: Benchmarking Cyber-Risk Quantification: Models, Use Cases and Outcomes

Hype Cycle for Cyber and IT Risk Management, 2021

Case Study: Criteria to Determine When to Perform Cyber-Risk Quantification

Case Study: Verizon's Cyber Risk Quantification Program

**About This Research**

This research is part of the 2021 Gartner Executive Retreat Series. The findings and analysis of this research are based on more than 60 interviews with SRM leaders and their teams, as well as a global benchmarking study on CRQ adoption rates, practices, outcomes, etc.

**Endnotes**

1. Top Security and Risk Management Trends 2021

2. 2021 Gartner Cyber Risk Quantification Survey
Position your IT organization for success. Explore these additional complimentary resources and tools for security and risk leaders:

**Webinar**
The Gartner Leadership Vision for 2022: Security and Risk Management
Prioritize your time and energy with top-level guidance based on our data-driven research.

**eBook**
Four Facets of Effective CISO Leadership
Discover how best-in-class cybersecurity leaders tackle their expanding remit.

**eBook**
3 Must-Haves in Your Cybersecurity Incident Response Plan
Improve your organization’s ability to be prepared for a cybersecurity incident.

**eBook**
Top Trends in Cybersecurity 2022
Explore the 12 trends shaping the future of digital business.

Already a client?
Get access to even more resources in your client portal. Log In
Get actionable, objective insight to deliver on your mission-critical priorities. Our expert guidance and tools enable faster, smarter decisions and stronger performance. Contact us to become a client:

**U.S.:** 1 855 811 7593

**International:** +44 (0) 3330 607 044

**Become a Client**

Learn more about Gartner for IT Leaders
gartner.com/en/information-technology

Stay connected to the latest insights  

© 2022 Gartner, Inc. All rights reserved. CM_GTS_1783750