MINNESOTA IT SERVICES

# Turning Risk into Reward with Cyber Risk Quantification


**State of Minnesota: Minnesota IT Services**

**Category:** Cybersecurity
**Initiated:** May 2022
**Completed:** April 2024

**Kendall Johnson**
Director of Communications
kendall.johnson@state.mn.us
(C) 651-334-1760

# Executive Summary

Minnesota IT Services (MNIT) is the information technology agency for Minnesota's executive branch, securing the data for 5.5 million Minnesotans. Led by the state's Chief Information Officer, MNIT sets IT strategy, direction, policies, and standards for enterprise IT leadership and planning. MNIT builds, maintains, and secures the state's IT infrastructure, applications, projects, and services. Additionally, MNIT delivers enterprise and local technology solutions for Minnesota state agencies that transform how government brings services to the people of Minnesota.

Minnesota's executive branch agencies do not have a unified method of cyber risk quantification (CRQ) for their high priority assets. As a result, agency leaders work in an environment where they:

- Have limited insights into the financial impacts of realized loss events.
- Must rely on subjective risk categorization (high/medium/low or red/yellow/green) to make risk-management decisions.
- Use current assessment methods that do not accurately forecast probability, magnitude, or frequency of loss events.
- Don't have insights into cost-effective, risk-remediation strategies.

Consequently, agency leaders' sole reliance on qualitative (subjective) risk reports results in inefficient identification and prioritization of risk and risk treatment planning.

MNIT identified a better way to make informed, strategic decisions around cybersecurity. We implemented an enterprise software tool built on the Factor Analysis of Information Risk (FAIR) model for quantitative cyber risk management solutions.

MNIT set up and piloted the tool over the past two years and launched it in April 2024. This FAIR-based risk quantification process helps relay business cybersecurity investments into the language of business and money, an approach that is somewhat unique for government.

This tool allowed MNIT to transform its processes for providing agency partners insight into how risks translate into business decisions.

**Why it matters:** Integrating a cyber risk quantification tool allows MNIT to translate cyber risk into business terms with data-driven metrics, so MNIT and business leadership can better understand, justify, and manage cybersecurity investment risks. In addition, having the ability to measure cyber risks is critical for making informed, strategic decisions. Because the tool can be used enterprise-wide, the cost savings it offers is a benefit to MNIT's partners and Minnesotans.

## CRQ Assessments

Showed one agency that implementing MFA would reduce the annualized loss exposure by **50% percent**.

Reduced the potential loss of just two information systems by **$3.18M**.

# Idea

State agencies do not have a unified method of cyber risk quantification, which limits their ability to make business decisions based on financial impacts of potential loss events.

Sole reliance on subjective data results in poorer outcomes for: prioritizing risk, implementing cost-effective mitigation plans, and addressing the needs of the business. These outcomes expose the agency to more severe financial loss (lower incident response) if a successful cyberattack were to occur.

Implementing a scalable, enterprise risk model such as CRQ, via the tool RiskLens, allows MNIT to standardize risk terminology, data collection criteria, measurement of risk factors, and reporting that speaks the language of business. This gives agency leaders a greater understanding of their agency's risk landscape and empowers them to make well-informed, risk-based decisions.

With it, MNIT uses an automated Security Scorecard process to give security teams and agency leaders insight into their security posture. This process also includes a forecasting capability to do "what if" scenarios, such as what if MNIT updated more systems, how would that improve our score?

CRQ is a framework that will help state agencies use data to evaluate cybersecurity risks and their potential financial impacts. This framework helps prioritize security investments based on the severity and likelihood of each threat, support compliance, and create a common language about security risks across an agency.

## CRQ helps MNIT and state agencies:

Promote the efficient use of data.

Align MNIT and state agency strategies to address business needs, while proactively managing risk.

Realize cost savings, process efficiencies, and operational performance gains for common products and services.

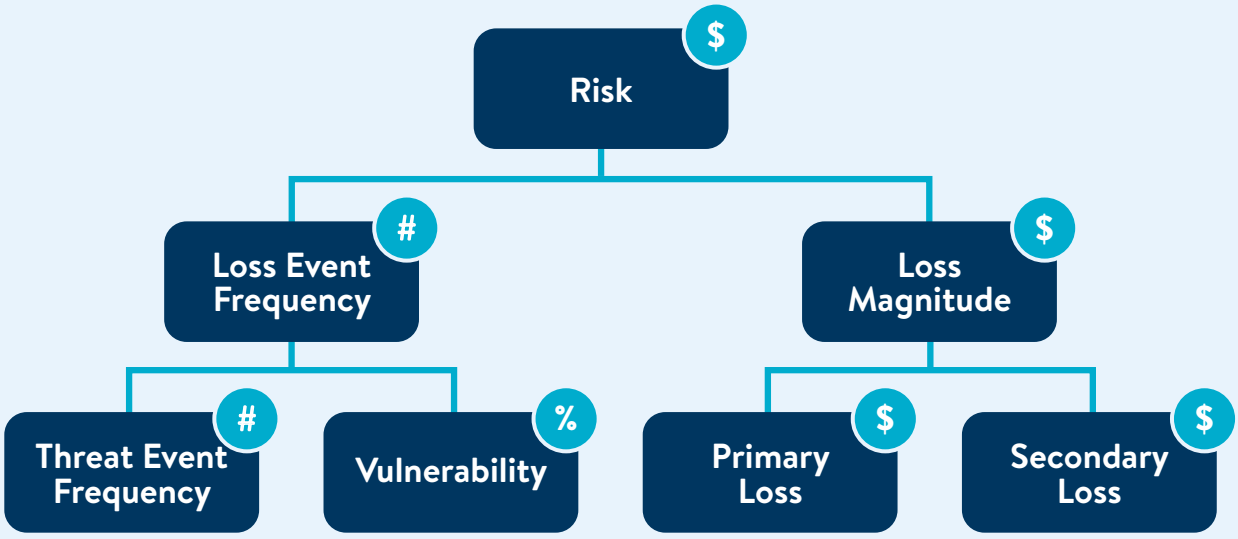
Reduce business impacts when cybersecurity events occur.

Use technology and data to increase efficiencies and improve decision-making.

The data used in CRQ is critical for conducting accurate cost-benefit analyses of security investments and forecasting monetary losses associated with loss events.

Using CRQ allows us to compare analyses in reverse, as well, to show what an asset's risk profile might be if a state agency removed one of its cybersecurity safeguards like a web application firewall (WAF). This is useful for justifying continued security investments. Additionally, CRQ can be used to justify why security doesn't need additional funding, saving agencies from unnecessary spending.

**Cyber Risk Quantification Framework**




# Implementation Approach

The status quo for risk assessment reporting was based on subjective interpretations of high/med/low or red/yellow/green scoring. MNIT technology leaders had to effectively communicate cybersecurity risks to agency business leaders, who are accountable for cybersecurity risk.

CRQ provides a means of communicating risk in a way that empowers leaders to make better-informed decisions to limit financial loss, show clear returns on security investments, and reassure citizens that their data is safe. Ensuring agency leaders understand their cybersecurity risk posture fosters a better partnership with MNIT, which has the responsibility to protect state systems and data. CRQ eliminates the subjectivity and allows MNIT to report in financial terms so that the business understands and prioritizes risks appropriately.

However, despite its importance and usefulness, CRQ is a relatively uncommon practice among other state cybersecurity entities. MNIT's adoption of CRQ sets Minnesota apart because the maturity of our risk management program is ahead of many other states.

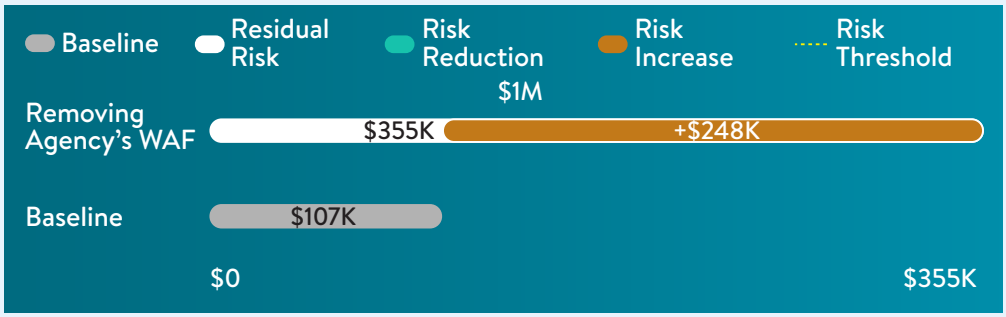
Because MNIT manages all information technology security practices for the State of Minnesota, MNIT strives to not only meet but exceed standard security measures to protect the information entrusted to us by Minnesotans. As a leader in the use of CRQ, MNIT has set an example for other states who are starting to implement their own CRQ program.

## Getting the Work Done

MNIT used an agile approach for project management, with frequent communications with key partners to improve data quality and maximize the value of risk assessment reporting for participating agencies.

RiskLens (and by extension, CRQ) aligns agencies with MNIT's 2023-2027 Strategic Plan by promoting the efficient use of data, addressing business needs while proactively managing risk, realizing cost savings, and bolstering whole-of-state cybersecurity. Reinforcing these objectives moves Minnesota closer to our goals of improved situational awareness and operational excellence.

## RiskLens Comparison Results





RiskLens comparison shows the change in risk exposure if the State of Minnesota were to **remove** a state agency's web application firewall (WAF) currently in place.

- Annual cost of cybersecurity safeguard is **$24,000**.
- Annual increase in loss exposure is **$248,000**.

MNIT conducted a one-year trial with 20 executive branch agencies as proof of concept. MNIT worked with these agencies to identify their highest priority applications. Then, MNIT identified the threats that posed the greatest risk to these applications. MNIT collected information that would help determine the financial, operational, and regulatory impact that a successful cyberattack would have against the application.

After obtaining sufficient data, MNIT used the CRQ tool to analyze the likelihood and magnitude of loss events, then prioritized them based on severity and criticality. The tool also calculates annualized loss expectancies and conducts cost-benefit analyses to determine the most effective mitigation strategies.

MNIT compiled its findings into quarterly reports, presented them to each agency's Business Information Security Officer (BISO) and Chief Business Technology Officer (CBTO), collected feedback, and adjusted the approach to maximize the value of our reports.

MNIT worked extensively with BISOs and business leaders to determine what their highest priority applications were, as well as what threats concerned them the most. Discussions with these groups helped us determine the scope of the assessments, probability, and potential impact if a successful cyberattack were to occur. MNIT also presented quarterly progress reports and gathered feedback from these groups. This frequent interaction allowed us to adjust the tool to maximize its value, as well as obtain buy-in from each agency.

MNIT made a conscious effort to involve agency BISOs and CBTOs through every iteration of the trial. MNIT engaged them for information on their agency's top assets and security concerns, held quarterly meetings to present asset loss expectancies, cost-benefit analyses, risk and safeguard comparisons, and make adjustments based on their feedback.

## Overcoming Roadblocks

MNIT experienced and overcame several obstacles as it moved forward in this project. During MNIT's procurement process, RiskLens was acquired by SAFE Security. MNIT negotiated a contract with SAFE Security that allowed us to retain the RiskLens tool MNIT used during the trial and enter a contract similar to what had been previously negotiated.

Internally, data quality and availability were the biggest roadblocks for conducting the assessments. Many of the inputs needed to produce actionable results were poorly documented or simply didn't exist. Obtaining these inputs required extensive time working with agency BISOs and business leaders.

These ongoing efforts highlight the importance of having good quality data available to get the most value from the CRQ tool. As a result, efforts are underway with the enterprise application portfolio management team to improve adoption of a centralized data repository and add data fields that will support CRQ assessments. The first set of updates took effect in May 2024.

# CRQ's Impact

Enabling agency leaders to make well-informed, risk-based decisions shows commitment to keeping citizens' data secure and being good stewards of taxpayer dollars. It minimizes the likelihood and impact of cyber threats if – or when – they occur, increasing the agency's ability to continue to provide services to Minnesotans.

Prior to this effort, Minnesota cabinet-level agencies had no method for cyber risk quantification. This CRQ effort helped solve the problem MNIT wanted to address. MNIT has seen proven success in multiple areas, including:

- **Risk exposure:** The impact of potential loss events is minimized.
- **Return on investment:** CRQ-driven cost-benefit analyses enable cost-effective security investments.
- **Cybersecurity posture:** Maturation of the state's risk management program.
- **Threat intelligence:** Enhanced ability to identify, prioritize, and mitigate threats.

Feedback from BISOs and CBTOs has been positive. They are excited to have their analysts trained, so they can begin conducting their own CRQ assessments.

The success of this effort can be seen in the ability of agencies to make more effective and cost-efficient security investments. Their ability to identify and mitigate threats will be improved, and the impact of loss events will be minimized.

This work was worthy of the initial investment because the potential cost-savings from effective risk prioritization, efficient security investments, and risk mitigation outweighs the total cost of ownership. The less tangible – but nonetheless equally as important – fact that MNIT is making Minnesotans' data more secure and maximizing uptime on the services they depend on makes this a worthy investment.

Implementing CRQ addresses three key priorities, as well as their collective objectives, related to customer experience, cybersecurity and operational excellence, and a connected culture.

## Results

### Risk Exposure

A assessment forecasted a $5.2 million annual loss exposure if an external threat actor were to gain a network foothold via phishing. The assessment found if the agency implemented multi-factor authentication, the annualized loss exposure could be **reduced by nearly 50%**, down to $2.4 million.

### ROI

During the pilot, the CRQ tool **provided over 10 times its value**, reducing the annualized loss expectancies of just two information systems by approximately $3.18 million.

### Cybersecurity Posture

CRQ allows us to review aggregate loss exposure for all agencies, identify agencies with the greatest loss magnitudes, and those that may exceed defined risk thresholds. Reporting can be as granular as reviewing all agencies' greatest forms of loss, most common threats, and the methods of attack that may be used against us.

### Threat Intelligence

Two high-priority information systems were identified as needing significant security investments. It was unclear which system should be prioritized, so the tool helped develop a loss event scenario for each asset. This revealed that the first had an annualized loss expectancy of $107,000, an average per-event loss of $1.3 million, with a rate of occurrence every six years. The second had an annualized loss expectancy of $295,000, an average per-event loss of $4.7 million, with a rate of occurrence every 11 years. This information allowed the agency to make a well-informed, risk-based decision about which system should be prioritized.

## Looking Ahead

Short-term, MNIT intends to train agency security analysts on how to use RiskLens, so each agency is capable of performing quantified risk assessments. A monthly community of practice will convene so analysts can share updates, ask questions, and review use-cases and results.

Long-term, MNIT will upgrade the tool to include API integrations with key data resources (Tenable, Veracode, Azure, AWS) to automate intelligence and information gathering, which will significantly decrease the time needed to conduct an assessment.