# Cloud Security Risk Management: State-wide Initiative For Financial Institution Security Reformation in Minnesota

UNIVERSITY OF MINNESOTA

**INET 4007 - Group 3**

**Azraf Daiyan, Jafar Gulet, Tyler Argent, Thomas Knickerbocker**

## Table of Contents

## Introduction

The board, led by the Governor, has presented a case to our CISO for formulating and executing comprehensive risk-reduction strategies for the State of Minnesota. This directive underscores the paramount importance of enhancing the state's cybersecurity posture, with a keen focus on minimizing vulnerabilities and potential threats. With a focus on the financial sector, our priority is the significant development of a practical solution for reducing risks within the State of Minnesota's finances.

In this organizational transition, key individuals have assumed pivotal roles, each with distinct responsibilities aimed at shaping the company's future. Jafar, as the VP of Marketing, is responsible for the institution's brand and communication strategies. Thomas is the institution's CISO and bears the responsibility of safeguarding the organization's digital assets. Tyler, as the VP of Operations, plays a central role in optimizing the institution's processes and workflows. Finally, Azraf, as the CIO, leads the company's technology strategy which includes overseeing IT infrastructuring, data management and other transformative initiatives related to the institution's digital assets.

## Team Roles and Definition

Thomas serves as the Chief Information Security Officer (CISO) within the represented financial institution in Minnesota. His primary responsibility is to ensure the safety and integrity of the organization's digital assets and information. This entails formulating and implementing comprehensive cybersecurity strategies to mitigate risks and protect against potential threats that could compromise the State of Minnesota's data and financial infrastructure. Thomas works to develop robust protocols, identify vulnerabilities, and create responsive strategies to enhance the cybersecurity posture of the state. Specific to the financial sector he represents, Thomas's role involves not only overseeing the technological aspects but also looking to establish best practices and protocols to ensure the highest level of security for the state's financial sector and other critical data systems.

Jafar serves as the VP of Marketing within the represented financial institution in Minnesota. He is responsible for developing and managing the application of marketing plans tailored to the specified requirements of the financial sector. This duty includes being aware of the state's procurement procedures, compliance standards, and cybersecurity environment. The VP is also responsible for proficiently conveying the benefits of the company's offerings to important state stakeholders, such as procurement officials, IT departments, and lawmakers. They also take the lead in creating ads and communications that are specifically targeted to the financial sector and emphasize security, dependability, and compliance with state laws. The position includes making sure that the company's products are positioned as ways to assist the state in strengthening its cyber posture and safeguarding its digital infrastructure. Specific to the financial sector he represents, Jafar is crucial for a financial institution as he drives brand visibility, customer acquisition, and product promotion, ultimately influencing the institution's growth and success.

Azraf serves as the Chief Information Officer (CIO) within the represented financial institution in Minnesota. As a CIO, his role involves strategic technology management, aligning IT initiatives with the organization's business objectives, and maintaining a secure and efficient IT infrastructure. Additionally, he is involved in leading IT teams, managing budgets, fostering vendor relationships, and being aware of opportunities to upgrade the current infrastructure based on new technological innovations that come out. He prioritizes innovation and data analytics to drive decision-making and ensure the organization remains competitive and technologically resilient. It is also important to note that a CIO and CISO should work together very closely as CIO’s provide the IT infrastructure that CISO’s rely on in order to be able to implement or revise new security measures. Specific to the financial sector he represents, Azraf is essential for a financial institution as he oversees IT strategy, security, and technological innovation, safeguarding sensitive data and ensuring the institution's competitiveness and operational efficiency.

Tyler serves as the Vice President of Operations within the represented financial institution in Minnesota. As the VP of Operations, he plays a crucial role in overseeing and optimizing the day-to-day activities that drive our organization's efficiency and effectiveness. His responsibilities include managing the supply chain, logistics, production, and quality control, ensuring that our processes run smoothly and cost-effectively. He's also charged with streamlining operations to enhance productivity, minimize waste, and meet customer demands. His focus extends to fostering a culture of continuous improvement, employee development, and safety within the operations team. By balancing strategic planning with hands-on management, he contributes to the organization's overall success, ensuring that our operations are aligned with our broader business objectives. Whilst not being directly involved in the IT infrastructure or IT work, the VP of Operations still plays an important role in establishing effective and efficient practices so that the rest of the organization such as the CIO, CISO, and VP of Marketing can be impactful in their positions. Specific to the financial sector he represents, Tyler is important as he ensures the efficient functioning of key processes, regulatory compliance, and customer satisfaction.

## Risk Identification Methodology

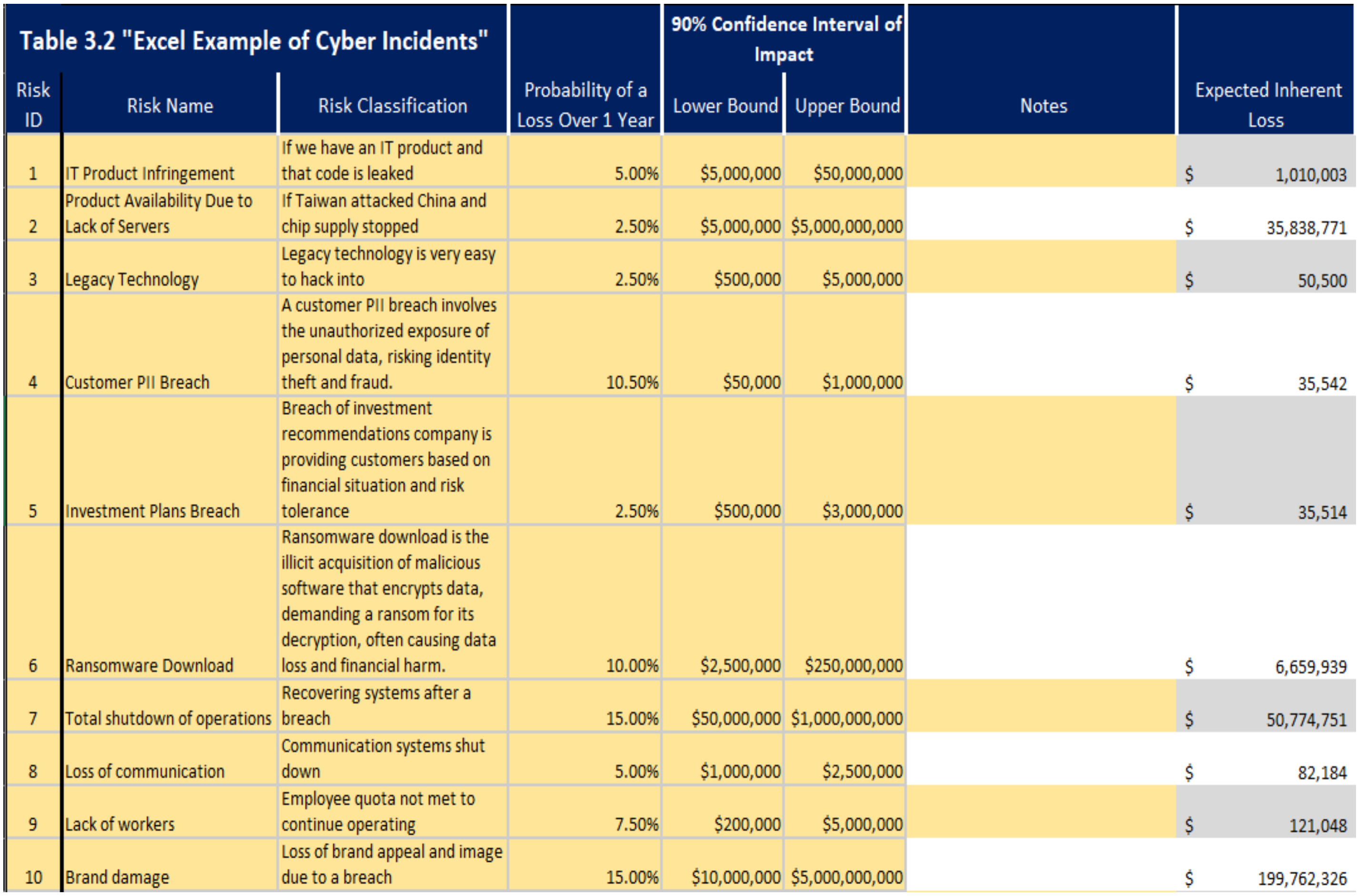

Table 3.2 "Excel Example of Cyber Incidents"

| Risk ID | Risk Name | Risk Classification | Probability of a Loss Over 1 Year | 90% Confidence Interval of Impact |  | Notes | Expected Inherent Loss |
|---|---|---|---|---|---|---|---|
|  |  |  |  | Lower Bound | Upper Bound |  |  |
| 1 | IT Product Infringement | If we have an IT product and that code is leaked | 5.00% | $5,000,000 | $50,000,000 |  | $ 1,010,003 |
| 2 | Product Availability Due to Lack of Servers | If Taiwan attacked China and chip supply stopped | 2.50% | $5,000,000 | $5,000,000,000 |  | $ 35,838,771 |
| 3 | Legacy Technology | Legacy technology is very easy to hack into | 2.50% | $500,000 | $5,000,000 |  | $ 50,500 |
| 4 | Customer PII Breach | A customer PII breach involves the unauthorized exposure of personal data, risking identity theft and fraud. | 10.50% | $50,000 | $1,000,000 |  | $ 35,542 |
| 5 | Investment Plans Breach | Breach of investment recommendations company is providing customers based on financial situation and risk tolerance | 2.50% | $500,000 | $3,000,000 |  | $ 35,514 |
| 6 | Ransomware Download | Ransomware download is the illicit acquisition of malicious software that encrypts data, demanding a ransom for its decryption, often causing data loss and financial harm. | 10.00% | $2,500,000 | $250,000,000 |  | $ 6,659,939 |
| 7 | Total shutdown of operations | Recovering systems after a breach | 15.00% | $50,000,000 | $1,000,000,000 |  | $ 50,774,751 |
| 8 | Loss of communication | Communication systems shut down | 5.00% | $1,000,000 | $2,500,000 |  | $ 82,184 |
| 9 | Lack of workers | Employee quota not met to continue operating | 7.50% | $200,000 | $5,000,000 |  | $ 121,048 |
| 10 | Brand damage | Loss of brand appeal and image due to a breach | 15.00% | $10,000,000 | $5,000,000,000 |  | $ 199,762,326 |

**Figure 1.1 -** 10 identified potential risks within the financial sector along with classification notes, annual probability loss, lower and upper bound of loss, as well as expected inherent loss.

## I. Probability of Loss Calculation Methodology

Calculating information regarding an annual potential loss can be tricky as there is not enough straightforward information to actually work with in a short research period. A valuable factor to consider for these calculations was that none of the identified risks are considered to be impossible as financial institutions are the target of cybercriminals often. It becomes highly unlikely more so when you consider that Minnesota is the housing location for one of 12 Federal Reserve Banks which again pushes the idea that it is impossible that one of these risks are likely to never occur. The risks that have lower probability loss percentages represent an educated guess that they are less likely to hurt the financial institution and are likely to be dealt with quickly with less damage. An example of this would be IT Product Infringement as that is not as likely to happen compared to some of the other risks that were identified and therefore the loss percentage is not as high as the others. An example of a harmful risk would be Total Shutdown of Operations as that would be extremely impactful towards the institution's likelihood to remain unscathed were all operations to suspend for a day. Bank shutdowns in general are very harmful towards the economic operations that occur on a day to day basis and therefore a shutdown from a cyberthreat could prove to be costly as well.

## II. Bound Calculation Methodology

Given the same criteria as above, providing rough estimations can be very tricky for a situation like this as there are many factors that were considered. For starters, the financial institution for the state is likely to have very costly bounds as they are in control of a lot of money. It becomes progressively tricky to calculate these bounds when also considering just how much money passes through a state as it has been currently quoted that Minnesota's current budget is around $48.6 billion dollars. It should also be noted that the current budget has shown a down trend since Fiscal 2022 which is why the values presented within the chart are lower expectations of result compared to the values potentially obtainable from a proper financial statement from the state banks. Because of this, the lower and upper bounds of loss are rather high for what you would expect of a banking institution, but the values make sense when you consider that we are measuring a state financial institution. Given a lack of information, it was concluded that the best approach, given the information presented, was to set the lower bounds to be similar to the upper bounds of smaller financial institutions within the state of Minnesota whilst setting the upper bounds to be similar to the level of the current state budget. This is represented well by the expected loss values being rather costly or not as costly when comparing how dangerous some of the risks are. An example of this can be seen in how costly total shutdown operations are as opposed to a legacy technology intrusion. Legacy technology is rather hard for newer cyberthreats to crack immediately which mitigates that risk as opposed to having a total shutdown which is part of safe practice for whenever there is a cyber intrusion.

## III. Top Three Identified Risks

Based on Figure 1.1, the three largest threats to the financial organization would be Total Shutdown of Operations, Product Availability Due to Lack of Servers, and Brand Damage. This is rather reasonable when you consider that all three of these risks bounce off one another and are capable of causing a domino effect where one starts the other. As the CIO, Azraf should be making sure that all the relevant infrastructure is set up effectively and safely so that Thomas, as the CISO, only has to worry about potential data leakage if the CIO doesn't respond to the lack of servers issue fast enough. In the event that there is a total suspension of operations temporarily during an intrusion and potential brand damage, The VP of Marketing as well as the VP of Operations should be making sure that the institution does not suffer incredible amounts of damage as well as making sure that operations are back up as fast as possible. Jafar and Tyler can do this by making sure that Thomas and Azraf are getting the right resources to block out the cyber intrusion and get the IT assets back to a safe state as fast as possible.

### Loss Exceedance Curve

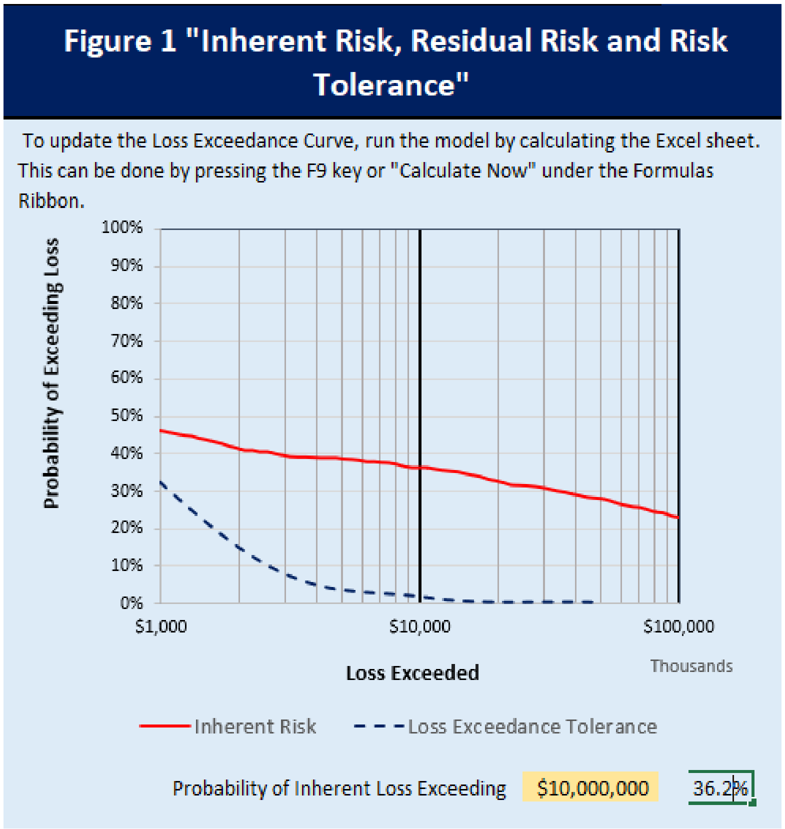

Figure 1 "Inherent Risk, Residual Risk and Risk Tolerance"

To update the Loss Exceedance Curve, run the model by calculating the Excel sheet. This can be done by pressing the F9 key or "Calculate Now" under the Formulas Ribbon.

Probability of Inherent Loss Exceeding $10,000,000 36.2%

**Figure 1.2 -** Loss Exceedance Curve for the 10 provided risks and the likelihood of passing the $10,000,000 range for expected loss. The current data presented a 36% chance of passing this threshold of loss.

### Funding Application and Result

Based on the loss exceedance curve, it is astounding that the likelihood of passing a cost value in the excess region of $10,000,000 is at 36 percent. Due to these results, it feels crucial that there is additional funding made available towards the following three risks to mitigate the loss exceeding range: Total Shutdown of Operations, Product Availability Due to Lack of Servers, and Brand Damage.  It should also be noted that another reason that estimating the funding necessary is difficult in this scenario is because there is not enough information actively present to be able to assume just how much value the financial institution holds and what the budget would look like for project related ventures. Rather than focusing on a value of funding towards these three risks, it seemed more valuable to simulate the change in the probability of inherent loss exceeding 10 million by showing the likelihood of annual loss percentage dropping.

| **Risk** | **Current Risk Probability** | **Risk Probability After Funding (Preferably)** |
|---|---|---|
| **Total Shutdown of Operations** | **15%** | **5%** |
| **Product Availability Due to Lack of Servers** | **2.5%** | **1%** |
| **Brand Damage** | **15%** | **5%** |

**Figure 2.1 -** Risk table showing the current risk probability and the preferred risk probability after funding is applied.

## I. Total Shutdown of Operations Updated Curve:

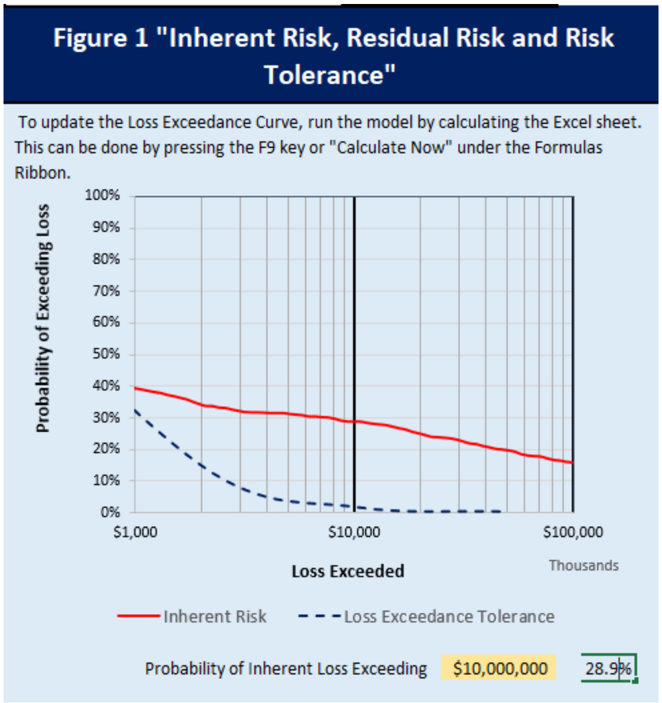

Figure 1 "Inherent Risk, Residual Risk and Risk Tolerance"

To update the Loss Exceedance Curve, run the model by calculating the Excel sheet. This can be done by pressing the F9 key or "Calculate Now" under the Formulas Ribbon.

Probability of Inherent Loss Exceeding $10,000,000 28.9%

**Figure 2.2 -** Loss Exceedance Curve after Total Shutdown of Operations funding adjustment

Based on figure 2.2, there is a major drop as there is now almost 8% less of a chance of exceeding the $10,000,000 range which could be seen from a funding application to bring the risk probability down from 15% to 5%. Realistically, it would be wiser to aim for a 1% risk probability, but for the sake of this simulation, a 10% decrease is viewed as a very large yet realistic drop in risk.

## II. Product Availability Due to Lack of Servers:

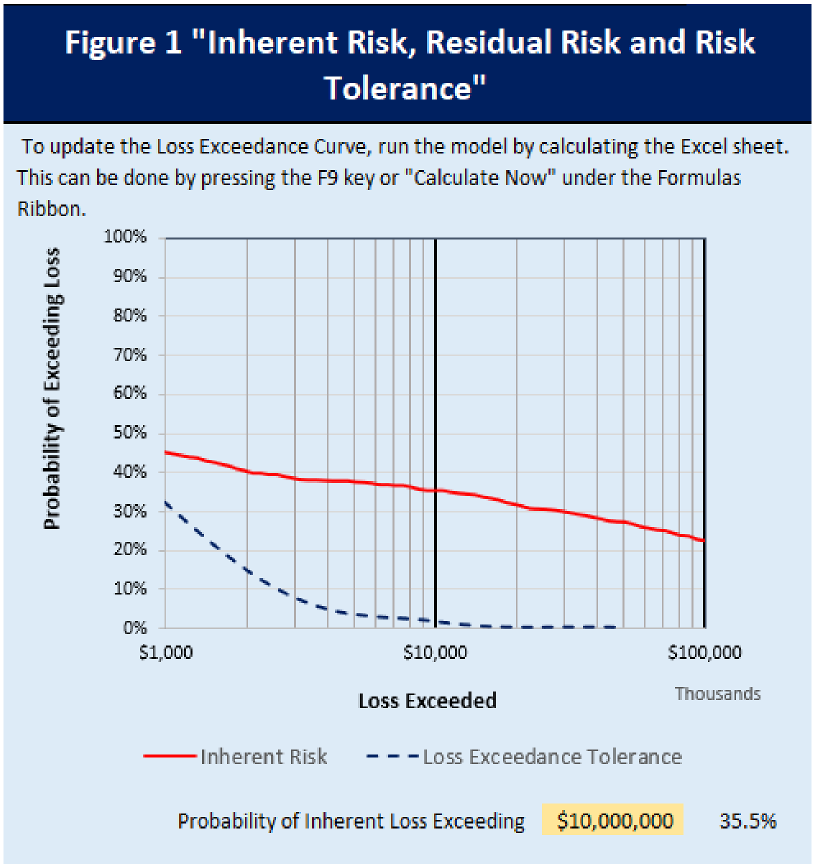

Figure 1 "Inherent Risk, Residual Risk and Risk Tolerance"

To update the Loss Exceedance Curve, run the model by calculating the Excel sheet. This can be done by pressing the F9 key or "Calculate Now" under the Formulas Ribbon.

Probability of Inherent Loss Exceeding $10,000,000 35.5%

**Figure 2.3 -** Loss Exceedance Curve after Lack of Servers funding adjustment

Based on figure 2.3, there is a drop of 4% less of a chance of exceeding the $10,000,000 range which could be seen from a funding application to bring the risk probability down from 10% to 1%. A drop of risk probability from 10 to 1% should still be viewed as realistic as it stays below our 10% bound of realism for this scenario, but it can be immediately noted that 32% is still relatively high and providing funding towards a Lack of Servers as opposed to Total Shutdown yielded less effectiveness by itself.

## III. Brand Damage Updated Curve

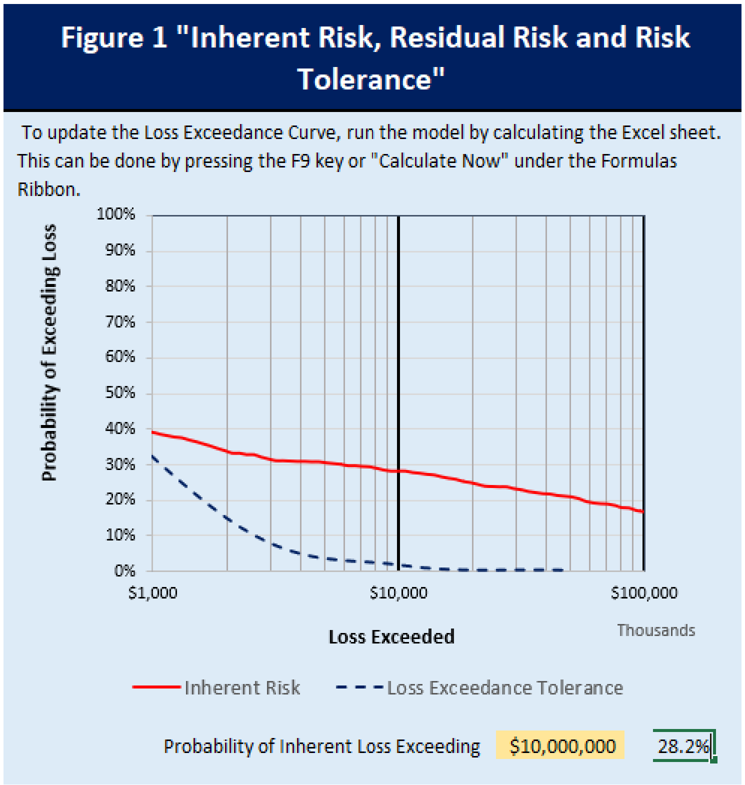

Figure 1 "Inherent Risk, Residual Risk and Risk Tolerance"

To update the Loss Exceedance Curve, run the model by calculating the Excel sheet. This can be done by pressing the F9 key or "Calculate Now" under the Formulas Ribbon.

Probability of Inherent Loss Exceeding $10,000,000 28.2%

**Figure 2.4 -** Loss Exceedance Curve after Brand Damage funding adjustment

Based on figure 2.4, there is a major drop as there is now almost 8% less of a chance of exceeding the $10,000,000 range which could be seen from a funding application to bring the risk probability down from 15% to 5%. Realistically, it would be wiser to aim for a 1% risk probability, but for the sake of this simulation, a 10% decrease is viewed as a very large yet realistic drop in risk. Again there seems to be an effectiveness in funding towards Brand Damage and Total Shutdown as opposed to funding towards a Lack of Servers.

## Summary

We outline a comprehensive Risk Identification Methodology for assessing potential risks within the financial sector, specifically using smaller Minnesota banks and the Minnesota Federal Reserve as a means of setting bounds for our assumptions. The Probability of Loss Calculation Methodology acknowledges the lack of straightforward data but highlights that none of the identified risks can be considered impossible in the context of frequent cyber threats targeting financial institutions across the world. Our analysis identified the following three risks to be the largest: Total Shutdown of Operations, Product Availability Due to Lack of Servers, and Brand Damage. These risks are interrelated, and it is recommended to coordinate efforts between relevant departments to mitigate them effectively. A Loss Exceedance Curve (Figure 1.2) illustrates the likelihood of exceeding a $10,000,000 loss threshold, with a current probability of 36%. Given the adjusted Loss Exceedance Curves (Figure 2.2 - 2.4) it would be reasonable to conclude that all of the funding should go towards resolving the risk of Brand Damage. Whilst that would bring the probability down to the lowest value out of the three adjusted risks after funding, it would be more efficient to instead dedicate the funding resources towards resolving the risk of a Total Shutdown of Operations. Funding adjustment towards Total Shutdown does have a higher probability than the one provided from adjusting Brand Damage, 28.9% versus 28.2%, it should be noted that providing funding towards Brand Damage does not mitigate the other two highlighted risks. In contrast, providing funding towards Total Shutdown of Operations closes down the likelihood of Brand Damage as well, thus resolving a potential domino effect issue that was present between the two risks. Because of provided understanding, it is important that the state governor is implored to provide more funding and resources towards the Total Shutdown of Operations risk.

## Works Cited

**_How Much Money Can a Bank Hold? | Wonderopolis_. (n.d.). Wonderopolis.org. https://wonderopolis.org/wonder/how-much-money-can-a-bank-hold#:~:text=Banks%20tend%20to%20keep%20only**

**_Minnesota_. Urban Institute. (n.d.). https://www.urban.org/policy-centers/cross-center-initiatives/state-and-local-finance-initiative/projects/state-fiscal-briefs/minnesota#:~:text=Minnesota's%20current%20budget&text=The%20budget%20included%20total%20spending,%2427%20billion%20in%20FY%202023.**

**Link To Spreadsheet: Spreadsheet**