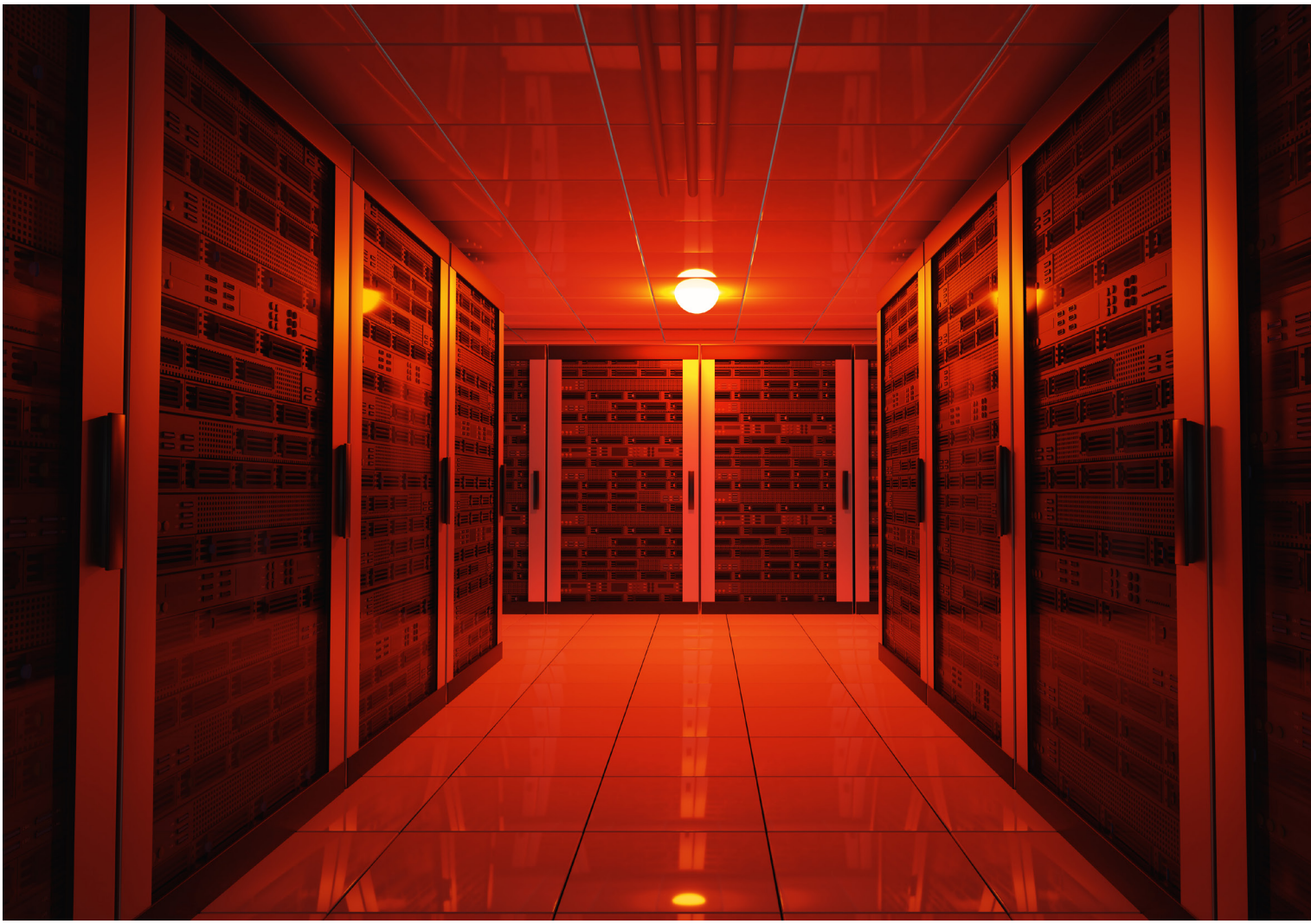
protiviti®

Face the Future with Confidence



Quantifying Cyber Disruption

The Impact of Ransomware

Internal Audit, Risk, Business & Technology Consulting

Executive Summary

2021 has been a record year for ransomware attacks — and it's not even over yet. Earlier in the year, a spate of attacks on critical infrastructure, including government institutions, caused the Biden administration to elevate the ransomware threat to a national security priority.

Facing a ransomware epidemic, boards are demanding that senior executives articulate the potential impact of ransomware to their organizations, as well as the steps taken to mitigate this risk. Chief information security officers have escalated calls for renewed investment in cybersecurity capabilities and new security technologies, requests that need to be balanced against the overall business objectives of their organizations.

A compelling case for increased investment in cybersecurity and prioritization of cyber resilience at the board level cannot be made without a solid understanding of an organization's vulnerabilities and its level of tolerance for cyber disruptions. In today's environment, a reactionary, tick-the-box approach no longer serves the interest of organizations — in fact, it may very well be catastrophic.

The objective of this paper is to demonstrate how organizations can quantify risks such as ransomware fully and accurately, and acquire the critical insights they need to build cyber resilience. Using a fictional entity, Mammoth Bank, as a case study, the paper demonstrates how a tried-and-tested method of risk quantification can be deployed to analyze ransomware risk. Through this detailed analysis, we estimate this fictional **$80 billion** bank's average annual exposure to ransomware to be **$10.2 million** and its per-event loss to be **$48 million** at minimum and **$266.3 million** in the worst-case scenario (90th percentile).

Ultimately, these insights will allow this fictional bank to determine its potential maximum disruption from a ransomware attack, assess whether or not current operations can withstand such an impact and make critical decisions to drive meaningful change.

[1] "Ransomware attacks continue to surge, hitting a 93% increase year over year," Check Point Research: https://blog.checkpoint.com/2021/06/14/ransomware-attacks-continue-to-surge-hitting-a-93-increase-year-over-year.

[2] The State of Ransomware 2021, Sophos, April 2021: https://secure2.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf.

To make a compelling case for increased investment in cybersecurity and prioritization of cyber threats at the board level, the guardians of information security need to understand their organizations' vulnerabilities and levels of tolerance for various cyber risks. A reactionary, tick-the-box approach no longer serves their interest - in fact, it may very well be catastrophic.

Sidebar 1: What Is Factor Analysis of Information Risk?

FAIR, or Factor Analysis of Information Risk[3], is an established method of risk quantification that can be used as a tool by an information security team to better analyze and communicate the risk of a cybersecurity incident to executive management. FAIR is the leading cyber risk quantification methodology due to its flexibility and wide industry adoption. FAIR can analyze many forms of loss, including confidentiality, availability and integrity, to help organizations understand the true impact of an event with wide-ranging impacts. Armed with facts and figures, the benefits of increased investment — and more important, the cost of inaction — can be presented clearly to executive management. The FAIR method is well-known and industry-accepted, particularly in the financial services industry.

Using FAIR, organizations can quantify the risk of individual loss events from ransomware and identify:

- The annualized expected and worst-case losses to the organization.
- The drivers of loss and most critical/impacted assets.
- Where additional investments in risk reduction will have the greatest impact.

[3] Fair Institute, What is FAIR?: www.fairinstitute.org/what-is-fair.

Case Study and Profile: Mammoth Bank

Mammoth Bank (the Bank) is a fictional bank created for use in this quantitative risk assessment exercise. In order to allow for the modeling of expected loss exposure due to a ransomware event, the following attributes will be assumed for the purpose of this exercise.

A Snapshot of Mammoth Bank

REVENUE	RETAIL CUSTOMERS	TRANSACTION VOLUME (PER HOUR)
$80B	35M	10K–40K

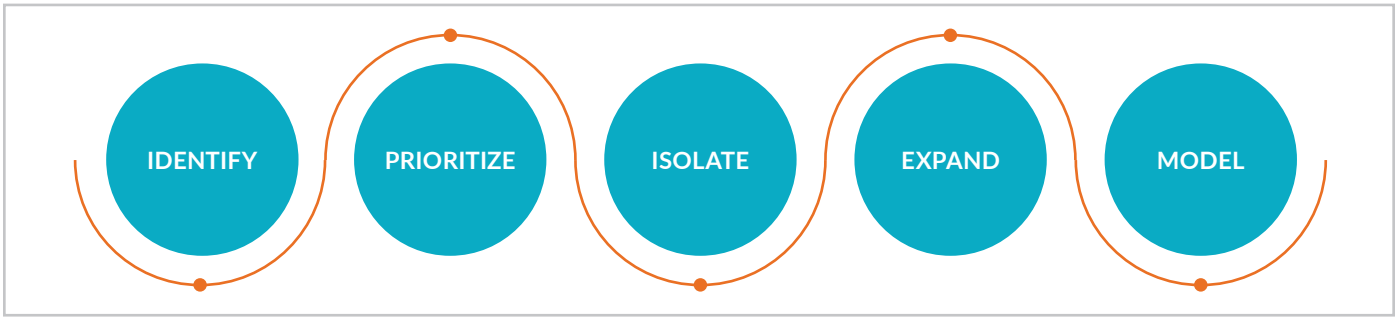
SERVICES

- Retail Banking
- Institutional Investment Management
- Clearing and Settlement
- Capital Markets

SCENARIO OVERVIEW

Through the methodology described below, Mammoth Bank will analyze the risk of a ransomware event perpetrated by a cybercriminal through a hacking incident. In this case, the Bank is interested in analyzing the risk of an attacker gaining access to the elevated privileges of an employee through the use of stolen credentials. The Bank will analyze the risks in relation to all loss effects (i.e., confidentiality, integrity and availability) by tracing the most probable actions and impacts for loss effect or asset.

• • • **Figure 1 — Protiviti's Approach to Quantifying a Ransomware Event**

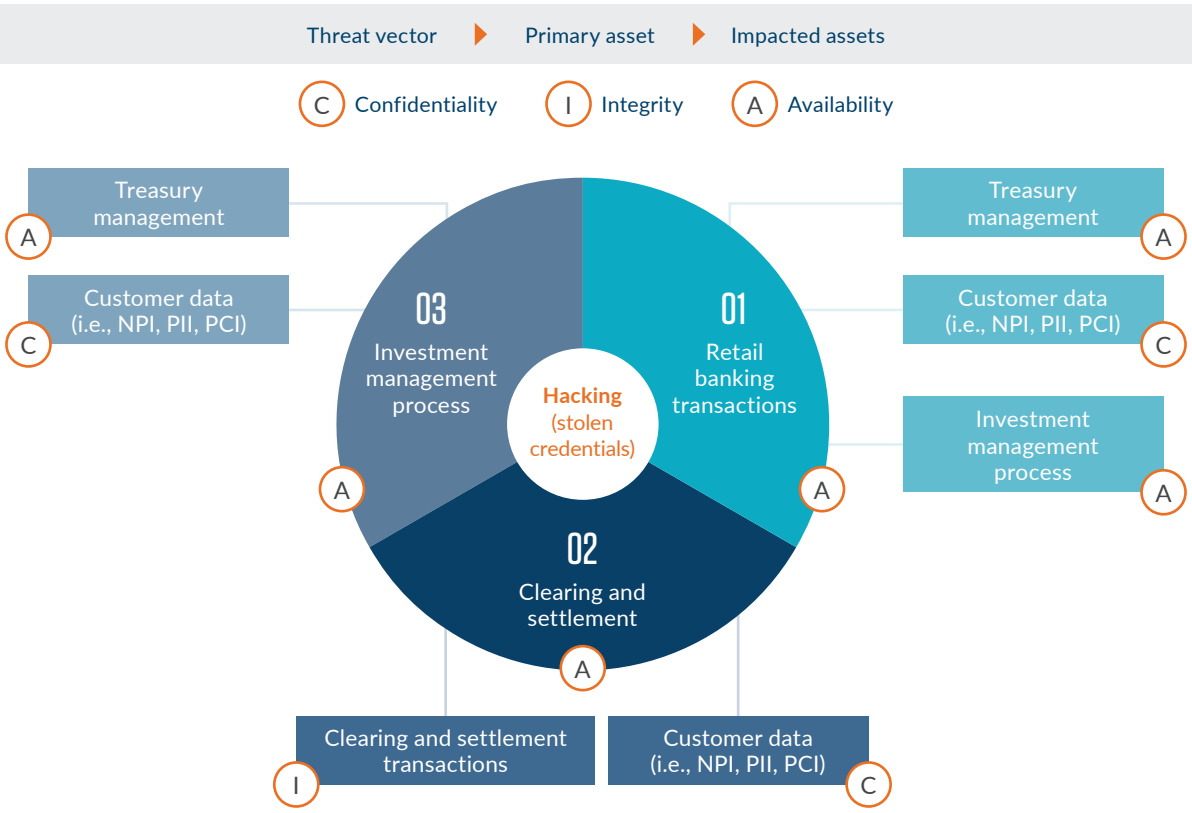


Approach to Quantification

By nature, the potential cost of a ransomware event can vary significantly, depending on the initial system impacted and how far the malware is able to spread across the organization's systems and cause disruption. Leveraging Protiviti's approach, Mammoth Bank was able to quantify the ransomware event by first identifying the likely points of entry and then quantifying both the initial impact and downstream system effects to provide a holistic picture of potential losses across the organization.

This approach, summarized in **Figure 1** above, uses existing risk quantification methods and provides a framework for aggregating and analyzing risks of multiple loss effects (i.e., confidentiality and availability risk) or multiple assets. This process begins with the most critical assets to the Bank and then determines what secondary or tertiary impacts could occur, similar to the approach outlined in **Figure 2**.

• • • Figure 2 — System Dependency Mapping and Scenario Identification



Each row can be analyzed as a discrete loss scenario.

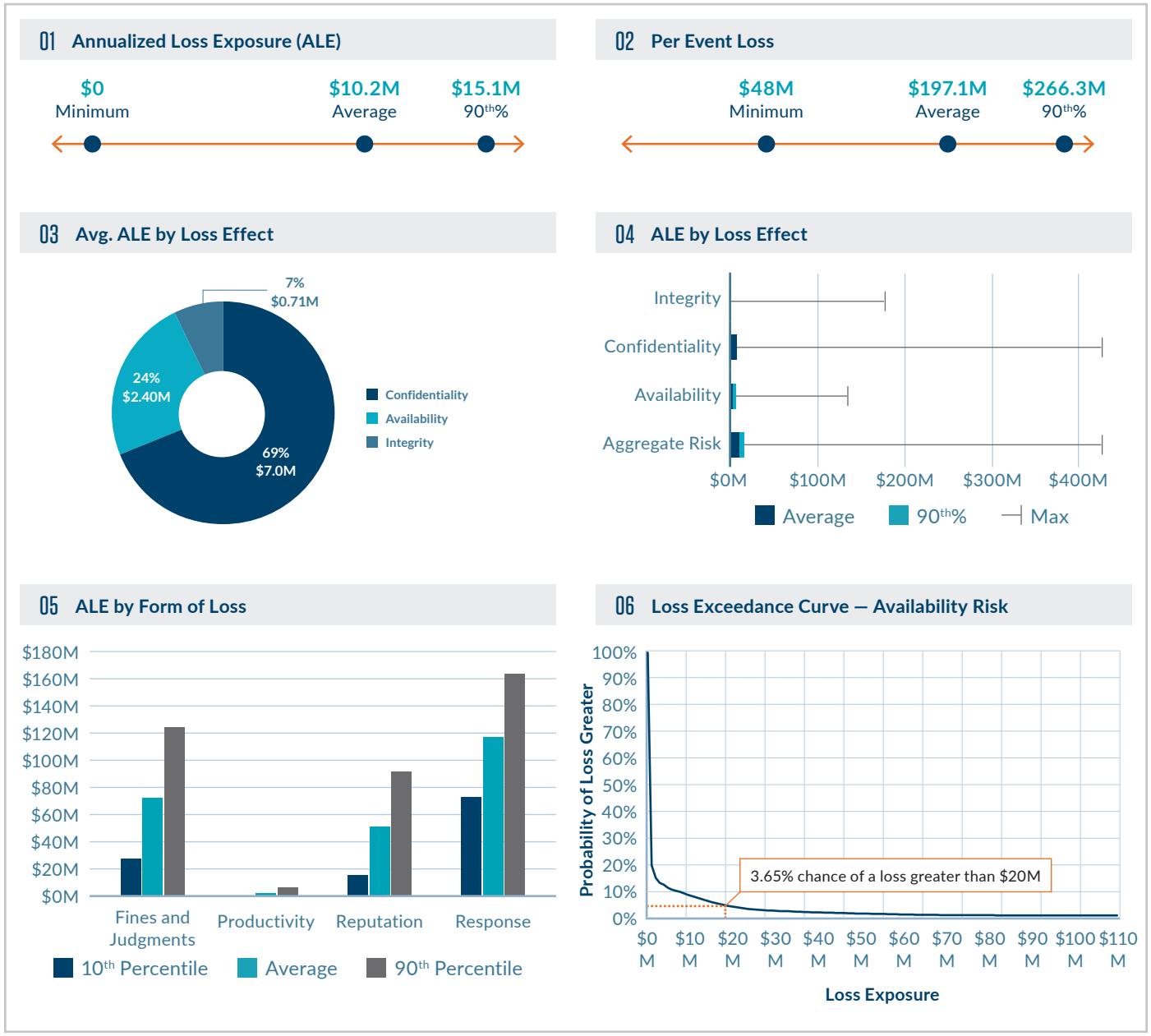
			Range of Potential Impact		
Threat Vector	Primary Asset	Loss Effect	Minimum	Most Likely	Maximum
Hacking (Stolen Credentials)	Retail Banking Transactions	A	Retail Banking Transactions	Retail Banking Transactions	1. External-Facing Retail and Investment 2. Internal Treasury Management
		C	None ($0)	Customer Data (i.e., NPI, PII, PCI)	Customer Data (i.e., NPI, PII, PCI)
	Clearing and Settlement	A	Clearing and Settlement	Clearing and Settlement	Clearing and Settlement
		C	None ($0)	Customer Data (i.e., NPI, PII, PCI)	Customer Data (i.e., NPI, PII, PCI)
		I	None ($0)	Clearing and Settlement Transactions	Clearing and Settlement Transactions
	Investment Management Process	A	Investment Management Process	Investment Management Process	All Holdings, Treasury and Investment Management

Translating From Dollars and Cents to Common Sense

Once data has been gathered at the asset level and at the aggregate level, Mammoth Bank now has a wealth of information on how a ransomware event could impact the organization. The question then becomes, what does it do with all this data?

In our scenario, the Bank uses the data to produce an array of metrics that can be presented in a dashboard format, as shown in **Figure 3** below, for executive management.

• • • **Figure 3 — Mammoth Bank Scenario Results**



Sidebar 2: Questions to Help Identify Critical Assets and Threats

- What are the organization's web-facing assets?
- Within the organization's respective industry, what assets are most frequently targeted by ransomware?
- How frequently are peers within the industry targeted by cybercriminals versus other industries?
- How effective are the organization's perimeter security controls, such as IDS/IPS and next-generation firewalls, and port hardening?
- What are the results of the organization's mock phishing exercises?
- How effective are the organization's email and endpoint AV/EDR controls at blocking users who unknowingly download ransomware to devices?

Refer to the **Appendix** for a detailed walk-through of our approach.

Annualized Loss Exposure

Overall risk from the Mammoth Bank scenario can be visualized by reviewing the annualized loss exposure (ALE). The ALE measure combines both the loss event frequency and loss magnitude into an annualized figure — representing loss exposure in any given year. It is a widely used measure in more than just the cyber risk quantification space.

There are several ALE measures that can be used, from minimum (i.e., a very good year) to 90th-percentile loss (i.e., a catastrophic but theoretically possible year). The amounts presented in Box 1 of the dashboard reporting demonstrate what overall loss from all forms of loss looks like for Mammoth Bank.

In this case, the Bank will use the data to better understand what its critical assets are and what the largest impacts from the event would be. The ALE by loss effect (Box 3 of the dashboard reporting) demonstrates that while availability of systems is important, the average ALE is mostly driven by a loss of confidentiality of customer data in these systems should the attacker choose to "name and shame" instead of simply holding the systems ransom.

This suggests that the Bank needs to invest more in encryption, obfuscation, data loss prevention or other technologies that could reduce the impact of data exfiltration of consumer data.

Finally, for a detailed view of ALE, the Bank can use a loss exceedance curve (such as the one presented in Box 6 of the dashboard reporting) to view the probability of loss of any dollar amount, up to the maximum.

Following is a summary of the advantages and disadvantages:

Advantages

- ALE factors in both loss event frequency and loss magnitude.
- ALE is easily translatable to management for forecasting purposes.

Disadvantages

- ALE can be skewed for low-frequency, high-magnitude events. Average and most-likely losses can in these cases appear very low, but additional measures (such as 90th-percentile and maximum loss) can be used to provide a more complete picture.

The ALE measure combines both the loss event frequency and loss magnitude into an annualized figure — representing loss exposure in any given year. It is a widely used measure in more than just the cyber risk quantification space.

Per-Event Loss

In addition to ALE, the Bank may choose to analyze its per-event loss. This amount can be very useful in understanding the impact of a ransomware event if it was to occur. It measures only the magnitude of the loss, not the likelihood of the event.

The Bank would consider using per-event loss amounts when managing impact tolerance. This measure can also be helpful in determining the level of cybersecurity insurance an organization should maintain. In Box 2 of the dashboard reporting presented, the Bank can see that the 90th-percentile per-event loss of this scenario is approximately **$266.3 million**. The Bank can use this number to gauge its remaining exposure if, in the worst case, this event occurred. The Bank can use this to answer the following questions:

- What would be the Bank's residual capital reserves before and after settlement of any cyber insurance claims?
- Would the Bank be able to meet capital requirements before any insurance claims are settled?
- Can the Bank demonstrate to regulators, such as the Federal Reserve, that it can manage potential harm to market participants and to overall market integrity to an acceptable maximum level in the event of a ransomware attack? This is particularly important for Mammoth Bank, which, in this case, is designated as a systemically important financial institution (SIFI) by the Financial Stability Board.

The advantages and disadvantages of a per-event loss analysis are summarized below.

Advantages

- Can be useful in situations where likelihood is low but the impact to the organization may be catastrophic. This is particularly useful in prioritizing assets for operational resilience purposes, a business impact analysis or cyber insurance purposes.

Disadvantages

- Per-event loss amounts exclude the likelihood of occurrence from the equation.
- The per-event loss analysis also ignores the potential for multiple follow-on events, like ransomware attacks that tend to target organizations after their initial breach becomes public.

Data Visualization

In addition to these important measures, the Bank can dissect and display losses in ways that allow more informed executive decision-making. Results can be viewed by loss effect (Box 4 of the dashboard reporting) or forms of loss (Box 5 of the dashboard reporting). In this case, the Bank can clearly see that loss of confidentiality is the most likely cause of any catastrophic event, with a maximum ALE of approximately **$415 million**. From the views by loss effect, it is evident that while fines and judgments (i.e., fines from OCC, SEC or FINRA) generate much of the loss, the Bank's internal costs associated with responding to both the initial event and then customer and regulatory actions are actually the largest driver of loss.

Sidebar 3: Types of Losses from Ransomware Events

- **Employee productivity losses —** Estimated employee productivity impacts and time to recover.
- **Lost revenues (i.e., interest and noninterest revenue) —** Interest revenue may not be lost due to a system outage in some cases, but a certain percentage of revenues for each hour of outage would create losses (i.e., consumers transferring their funds to another bank account, resulting in lost fees).
- **Reputation loss —** Percentages of likely lost customers as a result of inconveniences or perceived security weaknesses, valued based on the average lifetime value.
- **Fines and judgments —** Estimated range of potential fines and judgments incurred, based on the range of fines and judgments experienced by similar organizations from the regulators most likely to take action.
- **Response costs —** The costs of the organization responding to the initial event and any customer, partner or regulatory actions.
- **Direct losses —** Ransom demand payments offered in order to decrypt data and systems and restore availability.

Fines and judgments may not be in the control of the Bank, but the Bank can take actions to reduce response costs by automating certain failover activities or streamlining and testing its incident response plan regularly, among other options. As described in a Protiviti blog post[4], investments in the recover function of the NIST Cybersecurity Framework may be considered, given that organizations tend to invest the least in this function currently.

Because the Bank is regulated as a SIFI, it knows that it will be required to demonstrate its operational resilience capabilities in periodic stress tests or face additional scrutiny and capital requirements.

For reporting to management and the board, many of these measures can be helpful. A consolidated view of this can be achieved using a simplified, scenario-based risk register **(Figure 4)**. The view below clearly

[4] "Recover: The NIST Cybersecurity Framework's Outlier," Protiviti, May 6, 2021: https://tcblog.protiviti.com/2021/05/06/recover-the-nist-cybersecurity-frameworks-outlier/.

summarizes the risk to each individual asset, as well as to the Bank overall from the single scenario quantified in this exercise. This view measures each scenario by how the loss compares to the Bank's established risk tolerance thresholds.

For now, the Bank has populated the "triaged" qualitative values for the other scenarios, and as it continues to perform this exercise for additional scenarios, it can update those with the quantified values to provide further insights.

Figure 4 — Mammoth Bank Scenario-Based Risk Register View (Using Average ALE)

Threat	External Actor								
Initial Method	Hacking — Stolen Credentials			Ransomware (Malware)			Phishing/Pretexting		
Asset / Loss Effect	C	I	A	C	I	A	C	I	A
Retail Banking Transactions	N/A	N/A	$500K	N/A	N/A	L	N/A	N/A	L
Clearing and Settlement Transactions	N/A	$714K	$2M	N/A	L	L	N/A	H	M
Customer Data	$7M	N/A	N/A	M	N/A	N/A	H	N/A	N/A
Investment Management Process	N/A	N/A	$1.4M	N/A	N/A	L	N/A	N/A	H
Treasury Management Process	N/A	N/A	$900K	N/A	N/A	L	N/A	N/A	L
Aggregate Loss by Form	$7M	$714K	$2.4M	M	L	L	H	M	M
Aggregate Loss by Method	$10.2M			L			M		

What Your Organization Can Do Now

The ability to understand the business impacts of a ransomware event and clearly communicate that risk to executive management is critical for effective planning and response. With quantifiable information, organizations can make rational decisions and invest in additional controls to bring the quantified risks identified in line with management's risk appetite. Additionally, financial services organizations can make more logical business decisions related to capital requirements and comply with regulatory guidance related to impact tolerance.

Using FAIR, organizations can measure and more effectively manage risk related to ransomware. In addition to a traditional single-scenario view using FAIR, organizations can leverage a combined-asset view that escalates ALE calculations to match the behavior of a ransomware attack in a banking environment, which can start with a single system but quickly escalate to multiple systems and processes.

Organizations can operationalize this approach using a risk quantification engine that allows them to:

Use a repeatable mechanism for capturing the impacts to individual assets and the organization overall (i.e., loss tables).

Understand the linkages and dependencies between individual assets and visualize how many scenarios contribute to an ALE value.

View trends related to how the amounts of risk identified are changing over time.

Appendix: Mammoth Bank Ransomware Case Study — Analysis

1. IDENTIFY ASSETS AND THREATS

Risk assessment activities often begin with identification, and this effort is no different. The Bank first needs to establish what the landscape of potential threats and likely target assets would be.

Using a variety of industry data sources, the Bank narrows its focus to the cybercriminal, nation-state and hacktivist threat actors, all of which are external actors. In an actual risk analysis, there are opportunities for a privileged-insider attack or other threat actors to also take action that should also be considered.

The Bank must also categorize its list of assets. While it is important to identify all potentially impacted assets, emphasis is placed in this scenario on identifying those assets that could be the initial target of a ransomware attack. The Bank identifies the retail banking application and investment management application as likely targets because they are web-facing applications. The financial market utility used by the Bank is internally hosted and not a likely target for an initial attack by an external actor but will be considered in later steps of the analysis to determine the risk if ransomware spreads to infect more than just the initial system.

2. PRIORITIZE VECTORS AND LIKELY TARGETS

Using industry data and data from internal subject-matter experts, the Bank can triage the most likely threat methods and analyze them in relation to external web-facing assets. This can help identify which are most susceptible to, and most likely to experience, a future loss event. The Bank begins by identifying the range of outcomes likely to be experienced by the entity for that combination of asset and threat method before finally aggregating it to an entitywide view. To identify potential threat-actor movements and targets, the Bank leverages the MITRE ATT&CK® framework[5] and other sources of threat intelligence to establish a data-driven threat model of the likely attack pattern.

Using available industry data, the Bank has determined that the action most prevalent in attacks against the financial services industry involves brute-force attacks and use of stolen credentials as an entry into the environment. For example, in our fictional Mammoth Bank scenario, risk analysts can use data from the Bank's security operations center to determine if there are daily attempts at this type of attack against the Bank by a variety of groups. This data, based on criteria developed internally, indicates that such attempts occur at a very high frequency; however, due to controls in place, only 50% of these attacks are successful. While multifactor authentication is in use, it does not cover all remote access to systems. This loss is ultimately assessed to have a low likelihood of occurrence.

3. QUANTIFY IMPACTS TO SINGLE ASSETS

Starting with the most critical risks identified, the Bank can evaluate the potential loss if this single asset was impacted and then identify other assets that may be affected by an outage of the primary asset. The retail banking application is determined to be the most likely target and is initially rated as a very high risk to the organization. As a result, the Bank begins its analysis there.

For each loss identified, ranges of potential loss are constructed that represent the minimum, most likely and maximum loss for each potential form of loss. Taking its analysis of loss of availability as an example, Mammoth Bank has collected the following data applicable to the scenario:

[5] Enterprise Matrix, Mitre Corp.: https://attack.mitre.org/matrices/enterprise/

- An outage of the retail banking application caused by ransomware would last a minimum of one hour (the Bank's historical time frame in bringing systems back up following a major disruption) and up to a maximum of 16 hours. The Bank has never experienced an outage of 16 hours, but using calibrated estimation provided by subject-matter experts, it could not rule out (with 90% certainty) the possibility of an outage not occurring, even with existing controls. The organization mapped several responsive controls to this scenario, including:
  - Hot standby capabilities for all affected services, with data replicated to multiple processing sites in real time.
  - Availability of data backups at disaster recovery sites. Backups older than four hours are air-gapped, and certain copies are also archived, but there could be situations where ransomware not detected within four hours is replicated to the Bank's backup devices.
  - The above risk is partially mitigated by advanced threat detection and response tools deployed to the Bank's backup archives, but this would not be fully effective against novel ransomware threats.

  These controls, where effective, can reduce the outage duration, but due to gaps in some areas, the duration of the outage could be up to 16 hours.
- The Bank's business-line leadership estimated employee productivity impacts and time to recover using data collected from similar incidents at the Bank. These values can be applied broadly to similar assets.
- The Bank's annual revenues of $25 billion for consumer banking were used to develop an estimate of lost revenue for that application. Because the majority of revenue is interest income and would not be lost in a ransomware event, it is estimated that only 20% of revenues for each hour of outage would be truly lost (e.g., consumers choosing another bank to open an account or transfer funds).
- For reputation loss, data is obtained from the Bank's marketing team outlining the average customer lifetime value. For retail banking, this was determined based on average interest and fees (i.e., noninterest income) less costs for each customer. A similar range was used for global investment customers, though these customers generate more noninterest income and are generally more profitable for the Bank.
- An estimate of the range of potential fines and judgments incurred by the Bank in an actual loss event is developed based on the range of fines and judgments experienced by similar organizations from the regulators most likely to take action. Risk analysts at the Bank review historical fines levied by the Office of the Comptroller of the Currency (OCC), which ranged from $40 million to $400 million and would be more likely to occur only in the instance of an outage of eight or more hours. It is assumed these would be more likely if the Bank did not establish effective cybersecurity controls. In the event of a capital markets impact, such as if the ransomware moves laterally to global investments systems, additional regulators such as the Securities and Exchange Commission (SEC) or the Federal Reserve Bank may become involved, and fines could increase up to $4 billion, based on historical data, though this would be a very remote possibility.
- In this case, it is assumed a ransom demand payment is not facilitated, and the Bank is able to successfully recover systems without the attacker's involvement.

4. EXPAND ANALYSIS TO ENTIRE ORGANIZATION

Starting with the likeliest vectors and most critical assets, the Bank then identifies assets dependent on existing scoped assets. In this process, key dependencies of this application and potential additional loss events that could occur are outlined. While the Bank is primarily interested in a loss of availability of this application, there could also be losses of confidentiality and integrity that should be considered, based on actual attacker behavior previously discussed.

Assets are then mapped to identify what the potential best- and worst-case scenarios may be for each combination of threat method and initial target asset. For example, while the initial target asset may be retail banking transactions, if an outage of this asset could lead to additional business impacts, such as increased financing charges due to a longer order-to-cash cycle, or if the primary asset impacted is not effectively segmented from other assets, additional impacts may manifest themselves, such as an outage of the investment management process.

The Bank must also consider potential tertiary impacts. For example, the initial impact is likely to be availability, but certain ransomware events could result in losses of confidentiality (e.g., RAM scraping malware) or losses of integrity (i.e., data is modified in undetectable patterns during encryption) that may have separate loss effects.

While a significant component of the ransomware loss is related to availability, however, losses related to confidentiality could occur. There is a maximum of 90 million customer records within the various applications that could be impacted by ransomware, and while the Bank expects a confidentiality impact to only occur some of the time (one in three times at a maximum), the loss of even a single application's maximum records (20 million records) could incur additional reputational losses and additional regulator interest from the Financial Industry Regulatory Authority (FINRA), for example.

5. MODEL LOSSES

For an entitywide view, the Bank can then combine the results of its single-asset analysis into a broader scenario (**Table 1**), or a "combined-asset view." The Bank has already developed the loss tables at an asset level and can reuse this data to build ranges of loss if the event was to affect multiple assets across the organization. Potential impacts are grouped at the minimum, most likely and maximum, based on what the Bank expects would be affected a) each time (minimum) and b) in a likely scenario and based on how wide-ranging the effects could be in a worst-case scenario.

• • • Table 1 — Entitywide Ransomware Scenario Example

			Range of Potential Impact		
Threat Actor	Threat Vector	Loss Effect	Minimum	Most Likely	Maximum
Cybercriminal	Hacking (Stolen Credentials)	A	Retail Banking Transactions (Lowest Impact)	1. Retail Banking Transactions 2. Internal Treasury Management	1. External-Facing Retail and Investment 2. Internal Treasury Management 3. Clearing and Settlement
		C	None ($0)	Customer Data (i.e., NPI, PII, PCI) (Single System)	Customer Data (i.e., NPI, PII, PCI) (in Combined Systems)
		I	None ($0)	Clearing and Settlement Transactions	Clearing and Settlement Transactions

ABOUT PROTIVITI

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, analytics, governance, risk and internal audit through our network of more than 85 offices in over 25 countries.

Named to the 2021 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 60 percent of *Fortune* 1000 and 35 percent of *Fortune* Global 500 companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

CONTACTS

Terry Jost
Managing Director and Global Leader,
Security & Privacy
+1.469.965.6574
terry.jost@protiviti.com

Andrew Retrum
Managing Director,
Security & Privacy
+1.312.476.6353
andrew.retrum@protiviti.com

Daniel Stone
Associate Director
Security & Privacy
+1.404.926.4325
daniel.stone@protiviti.com

Tim Kelly
Senior Manager
Security & Privacy
+1.815.600.3567
tim.kelly@protiviti.com

THE AMERICAS

UNITED STATES
Alexandria, VA
Atlanta, GA
Austin, TX
Baltimore, MD
Boston, MA
Charlotte, NC
Chicago, IL
Cincinnati, OH
Cleveland, OH
Columbus, OH
Dallas, TX
Denver, CO
Ft. Lauderdale, FL
Houston, TX
Indianapolis, IN
Irvine, CA
Kansas City, KS
Los Angeles, CA
Milwaukee, WI
Minneapolis, MN
Nashville, TN
New York, NY
Orlando, FL
Philadelphia, PA
Phoenix, AZ
Pittsburgh, PA
Portland, OR
Richmond, VA
Sacramento, CA
Salt Lake City, UT
San Francisco, CA
San Jose, CA
Seattle, WA
Stamford, CT
St. Louis, MO
Tampa, FL
Washington, D.C.
Winchester, VA
Woodbridge, NJ

ARGENTINA*
Buenos Aires

BRAZIL*
Belo Horizonte*
Rio de Janeiro
São Paulo

CANADA
Toronto

CHILE*
Santiago

COLOMBIA*
Bogota

MEXICO*
Mexico City

PERU*
Lima

VENEZUELA*
Caracas

EUROPE, MIDDLE EAST & AFRICA

BULGARIA
Sofia

FRANCE
Paris

GERMANY
Berlin
Dusseldorf
Frankfurt
Munich

ITALY
Milan
Rome
Turin

THE NETHERLANDS
Amsterdam

SWITZERLAND
Zurich

UNITED KINGDOM
Birmingham
Bristol
Leeds
London
Manchester
Milton Keynes
Swindon

BAHRAIN*
Manama

KUWAIT*
Kuwait City

OMAN*
Muscat

QATAR*
Doha

SAUDI ARABIA*
Riyadh

UNITED ARAB EMIRATES*
Abu Dhabi
Dubai

EGYPT*
Cairo

SOUTH AFRICA *
Durban
Johannesburg

ASIA-PACIFIC

AUSTRALIA
Brisbane
Canberra
Melbourne
Sydney

CHINA
Beijing
Hong Kong
Shanghai
Shenzhen

INDIA*
Bengaluru
Chennai
Hyderabad
Kolkata
Mumbai
New Delhi

JAPAN
Osaka
Tokyo

SINGAPORE
Singapore

*MEMBER FIRM

protiviti®