Contents

Executive summary

Risk Assessment Foundation
Accurate risk assessment relies heavily on precise values and figures tailored to our organization. While we have currently harnessed industry averages as a foundation for our calculations, it is imperative to note that these are broad benchmarks. They serve as a starting point, with the understanding that direct consultations with our organizational leadership and experts will provide an enhanced layer of specificity. Our model remains flexible, designed to incorporate refined figures for a more precise output.

Historical
Past incidents within the industry offer insightful lessons. Our analysis included three notable cases to illustrate varied strategies and outcomes:

- Humana and Cigna – Both entities abstained from paying ransoms. Their decisions led to financial setbacks of $100 million and $50 million, respectively. (McKeon, 2021)
- Aetna – They opted for a different route by paying a ransom of $300,000. However, it's crucial to note that only a segment of their data was under encryption. (Intraprise Health, 2023) (Rosenzweig, 2023).

These historical scenarios underline the profound financial disparities based on chosen strategies. Our report delves into an analysis that details potential outcomes if the ransom is paid or if the organization decides against it.

Response and Recovery
The way an organization confronts and recuperates from a ransomware attack has overarching implications on total losses. Our detailed analysis not only concentrates on ransomware risk metrics but also emphasizes the overarching security posture. This includes:

- Incident Response Plan which has a step-by-step protocol for immediate action during and after a security breach.
- Data Recovery Plan to ensure data integrity and swift recovery post-incident.
- Business Continuity Plan that includes strategies to maintain business operations during and after an attack.

Our assessment emphasizes that the efficacy of these plans directly correlates to the severity of the organizational impact. Their meticulous crafting and execution are paramount in both risk mitigation and operational resilience.

While our current assessment provides a broad picture, refining it with more tailored figures from in-house discussions will solidify our strategic preparedness. We remain committed to not only understanding potential risks but also strengthening our response mechanisms.

Glossary

Action: An act taken against an Asset by a Threat Agent. Requires first that contact occurs between the Asset and Threat Agent.

Asset: The information, information system, or information system component that is breached or impaired by the Threat Agent in a manner whereby its value is diminished or the act introduces liability to the Primary Stakeholder.

Contact Event: Occurs when a Threat Agent establishes a physical or virtual (e.g., network) connection to an Asset.

Contact Frequency (CF): The probable frequency, within a given timeframe, that a Threat Agent will come into contact with an Asset.

Control: Any person, policy, process, or technology that has the potential to reduce the Loss Event Frequency (LEF) – Loss Prevention Controls – and/or Loss Magnitude (LM) – Loss Mitigation Controls.

FAIR: Factor Analysis of Information Risk.

Loss Event: Occurs when a Threat Agent's action (Threat Event) is successful in breaching or impairing an Asset.

Loss Event Frequency (LEF): The probable frequency, within a given timeframe, that a Threat Agent will inflict harm upon an Asset.

Loss Flow: The structured decomposition of how losses materialize when a Loss Event occurs.

Loss Magnitude (LM): The probable magnitude of loss resulting from a Loss Event.

Loss Scenario: The story of loss that forms a sentence from the perspective of the Primary Stakeholder.

Primary Stakeholder: The person or organization that owns or is accountable for an Asset.

Probability of Action (PoA): The probability that a Threat Agent will act against an Asset once contact occurs.

Resistance Strength (RS): The strength of a Control as compared to the probable level of force (as embodied by the time, resources, and technological capability; measured as a percentile) that a Threat Agent is capable of applying against an Asset.

Risk: The probable frequency and probable magnitude of future loss.

Risk Analysis: The process to comprehend the nature of risk and determine the level of risk. [Source: ISO Guide 73:2009]

Risk Assessment: The overall process of risk identification, risk analysis, and risk evaluation. [Source: ISO Guide 73:2009]

Risk Factors: The individual components that determine risk, including Loss Event Frequency, Loss Magnitude, Threat Event Frequency, etc.

Risk Management: Coordinated activities to direct and control an organization with regard to risk. [Source: ISO Guide 73:2009]

Secondary Stakeholder: Individuals or organizations that may be affected by events that occur to Assets outside of their control. For example, consumers are Secondary Stakeholders in a scenario where their personal private information may be inappropriately disclosed or stolen.

Threat: Anything that is capable of acting in a manner resulting in harm to an Asset and/or organization; for example, acts of God (weather, geological events, etc.), malicious actors, errors, failures.

Threat Agent: Any agent (e.g., object, substance, human) that is capable of acting against an Asset in a manner that can result in harm.

Threat Capability (TCap): The probable level of force (as embodied by the time, resources, and technological capability) that a Threat Agent is capable of applying against an Asset.

Threat Community: A subset of the overall Threat Agent population that shares key characteristics.

Threat Event: Occurs when a Threat Agent acts against an Asset.

Threat Event Frequency (TEF): The probable frequency, within a given timeframe, that a Threat Agent will act against an Asset.

Vulnerability (Vuln): The probability that a Threat Event will become a Loss Event; probability that Threat Capability is greater than Resistance Strength. (Synonym: Susceptibility)

Analysis

A. The Scenario

This is a risk assessment using the FAIR framework for Placebo Inc due to the risk of ransomware.

B. Identify scenario components

a. Identify the asset at risk

The primary asset at risk within Placebo Inc. due to ransomware is the data housed within the organization's servers.

b. Identify the threat community under consideration

Placebo Inc., given its nature of operations in the health insurance sector, is exposed to several threats. After a detailed examination, three primary threat communities were identified as having the potential and motive for orchestrating a ransomware attack:

- Advanced Persistent Threat (APT) groups
- Organized Crime Groups
- Nation-State Attackers.

C. Evaluate Loss Event Frequency (LEF)

a. Estimate the probable Threat Event Frequency (TEF)

Based on the data, the Threat Event Frequency (TEF) is calculated by considering the frequency with which our identified threat communities are likely to exploit vectors granting them access to Placebo Inc's server data.

b. Estimate the Threat Capability (TCap)

The capability of threats varies, ranging from trivial actors to sophisticated cybercriminals. Based on our analysis, ransomware deployment and sophistication is expected to be between 50% (minimum) to 90% (maximum), with the most probable capability estimated at 75%.

c. Estimate Control Strength (CS)

Placebo Inc. has incorporated several measures to bolster its defense mechanisms, ranging from spam filters to software patches. The Resistance Strength metric takes into account robust security practices which bolster defenses against ransomware threats.

d. Derive Vulnerability (Vuln)

The vulnerability is a function of Threat Capability and Control Strength. Given the identified control strengths and the spectrum of threat capabilities, vulnerability varies.

e. Derive Loss Event Frequency (LEF)

This is calculated by multiplying the COF by the POA, which results in the total expected frequency of successful ransomware attacks within a year.

D. Evaluate Probable Loss Magnitude (PLM):

Once a threat agent acts upon an asset, the first phase of the loss event begins and we refer to this as Primary Loss. The owner of the affected asset is referred to as the Primary Stakeholder. The second phase of the loss event occurs as a result of the Secondary Stakeholders reacting negatively to the Primary Loss, the “fallout” of the loss. Loss magnitude is derived from both Primary and Secondary Loss values. Losses in both categories fall under six types: productivity, response, replacement, fines and judgments, competitive advantage, and reputation. However, productivity, response, and replacement are typically forms of Primary Loss, and response, fines and judgments, competitive advantage, and reputation are typically forms of Secondary Loss. Secondary loss presents itself as, but is not limited to: regulatory fines, settlement fines, contractual fines, stock price reductions, increased insurance premiums, and losses due to market share. The Secondary Loss Event Frequency is the likelihood, expressed in a percentage, that the primary loss will trigger a secondary loss event. This variable tends to vary based on the type of event, however, when an organization specifically deals with sensitive customer information, the likelihood of a secondary event being triggered is almost always. Freund & Jones (2014, p. 156).

a. Estimate Primary Loss

We gathered data from the health insurance agency, including data from historical threat events and their aftermath.

b. Estimate Secondary Loss

We estimated the secondary loss magnitude by gathering data based on loss exposure due to fines imposed on health insurance organizations that experienced a data breach, and the resulting cost of cyber security insurance and increase in premiums. By reviewing the largest data breaches affecting the health insurance organization, we assumed that the maximum loss exposure due to fines would be $64.2 million, the most likely would be $33.7 million, and minimum would be $3.2 million. Additionally, we assumed that the maximum loss exposure due to insurance premiums would be $1.506 million, the most likely would be $612K, and the minimum would be $48K.

Due to the nature and level of sensitivity of the data Placebo Inc. deals with on a daily basis, the likelihood of a secondary event was extremely high. Thus, resulting in the following: a maximum secondary loss event frequency of 99%, a likely secondary loss event frequency of 97%, and a minimum secondary loss event frequency of 95%.

E. Evaluate Vulnerability (Vuln):

a. Threat Capability

The vulnerability metric is the probability that a threat event will become a loss event. In this analysis we analyzed vulnerability at the threat capability and resistance strength levels to determine vulnerability.

This analysis is looking at the threat event of ransomware. Ransomware itself is readily available as a ready to deploy malware but variants can either be re-coded or made from scratch which in of itself warrants differing levels within the capability continuum. Ransomware is not an initial action taken by threat actors and is normally a secondary action taken after an initial compromise has taken place. This initial action is also considered within the capability continuum. The threat capability we analyze represents a collaboration of these two items and where they would meet on the capability continuum. The data points that inform this analysis are derived from reputable reports and subject matter experts such as Mitre, CISA, and Verizon. Most likely we will be at risk of ransomware attacks from the 75th percentile of threat actors with 50% and 90% representing the minimum and maximum percentiles we would be at risk from.

b. Resistance Strength

The resistance strength metric considers our security posture against ransomware attacks based on industry guidelines and best practices from NIST, CISA, Mitre, and Verizon. These practices are implemented into our security strategy to protect assets from ransomware. Use of cyber resiliency practices work to curtail losses by allowing operations to continue during an attack. The analysis thus incorporates this and it is most likely that a threat actor at the 85th percentile could circumvent controls to successfully begin to launch a ransomware attack. Because of the various methods that ransomware could be delivered, some being trivial, we see the minimum at 60% which represents user error such as falling victim to phishing, compromised device, or compromised credentials.

Recommended actions

1. Enhance Cyber Awareness
   Placebo Inc. should continue to prioritize regular software and firmware updates, maintain stringent backup protocols, and conduct periodic security audits to ensure no vulnerabilities are left unaddressed.

2. Training
   Given that many attacks exploit human errors, regular training programs should be conducted to educate employees about the latest threats and how to identify and report suspicious activities.

3. Incident Response Plan
   An incident response plan should be developed, tested, and regularly updated. This plan would provide a roadmap for navigating potential breaches and minimizing damage.

4. Insurance Review
   It would be important to review the company's cyber insurance policy to ensure it provides adequate coverage in the event of a breach.

5. Engage with Regulatory Bodies
   Maintain an open channel with regulatory bodies to ensure Placebo Inc. remains compliant with all industry standards and regulations.

6. Invest in Advanced Threat Detection
   Implementing advanced threat detection solutions that employ machine learning and artificial intelligence can provide proactive defense mechanisms against sophisticated threats.

References

Alder, S. A. (2017, February 2). $3.2 Million HIPAA Civil Monetary Penalty for Children's Medical Center of Dallas. Retrieved from https://www.hipaajournal.com/3-2-million-hipaa-civil-monetary-penalty-childrens-medical-center-dallas-8673/

Alder, S. A. (2020, October 1). Anthem Inc. Settles State Attorneys General Data Breach Investigations and Pays $48.2 Million in Penalties. Retrieved from https://www.hipaajournal.com/anthem-inc-settles-state-attorneys-general-data-breach-investigations-and-pays-48-2-million-in-penalties/

Burgard, M. (2023, August 19). Cyber Incident Response: The Real Cost Of Not Having A Plan Or Cyber Insurance. Marconet. https://www.marconet.com/blog/cyber-incident-response

Coveware. (2022). Q4 2021 Ransomware Marketplace Trends Report. https://www.coveware.com/ransomware-quarterly-reports

Cyber Insurance: Insurers and policyholders face challenges in an evolving market. (2021, May 20). U.S. GAO. https://www.gao.gov/products/gao-21-477

Freund, J., & Jones, J. (2014). Measuring and managing information risk: A FAIR Approach. Butterworth-Heinemann.

Guinan, S. (2023, July 28). Largest Health Insurance Companies of 2023. Valuepenguin. https://www.valuepenguin.com/largest-health-insurance-companies

Health Cyber: Ransomware Resource Center. (n.d.). https://healthcyber.mitre.org/

HIPAA Journal. (2022). Top 10 industries targeted by ransomware in 2022. https://www.statista.com/statistics/1323599/us-most-targeted-industries-by-ransomware-attacks/

Intraprise Health. (2023). Cybersecurity Nightmares: The cost of healthcare cyberattacks in 2023. Intraprise Health. https://intraprisehealth.com/the-cost-of-cyberattacks-in-healthcare/

James, N. (2023, August 4). AWS Penetration Testing report: Everything you should know! Astra Security Blog. https://www.getastra.com/blog/security-audit/phishing-attack-statistics/

Jansen, B. (2023). 14+ Malvertising Statistics, Facts & Trends (2023). vpnAlert. https://vpnalert.com/resources/malvertising-statistics/

McGinn, M. (2023, July 31). Number of Servers. Quora. https://www.quora.com/How-many-servers-does-an-enterprise-have

McKeon, J. (2021, October 27). Third-Party vendor ransomware attack impacts Humana, anthem members. HealthITSecurity. https://healthitsecurity.com/news/third-party-vendor-ransomware-attack-impacts-humana-anthem-members

Meyer, H. (2023, March 30). The 10 biggest penalties for HIPAA violations. Providertech. https://www.providertech.com/the-ten-biggest-penalties-for-hipaa-violations/

Mindanao, K. (2023, August 2). How Much Does a Server Cost in 2023? (All Factors Explained) [Updated]. Itsasap. https://www.itsasap.com/blog/server-cost

Molina Healthcare. (n.d.). https://www.molinahealthcare.com/members/common/en-us/abtmolina/compinfo/compinfo.aspx

Private industry compensation costs $35.96 per hour worked, health insurance cost $2.73, June 2020. (2020, September 22). U.S. Bureau of Labor Statistics. https://www.bls.gov/opub/ted/2020/private-industry-compensation-costs-35-96-per-hour-worked-health-insurance-cost-2-73-june-2020.htm

Ransomware FAQs | CISA. (n.d.). Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/stopransomware/ransomware-faqs

Raza, M. (2023, February 14). Social Engineering Attacks: The 4 Stage Lifecycle & Common Techniques. Splunk-Blogs. https://www.splunk.com/en_us/blog/learn/social-engineering-attacks.html

Rosenzweig, R. (2023, March 6). As cyber attacks on health care soar, so does the cost of cyber insurance. Axios. Retrieved from https://www.axios.com/2023/03/06/cyber-attacks-cost-of-cyber-insurance

UnitedHealthCare. (n.d.). https://www.unitedhealthgroup.com/people-and-businesses/businesses/unitedhealthcare.html

Verizon. (2022). 2022 Data Breach Investigations Report. https://www.verizon.com/business/resources/reports/dbir/

Why Does Cyber Insurance Cost So Much? (2023, January 10). Hylant. https://hylant.com/insights/blog/cyber-insurance-cost

Appendix A - Workings

All references are found in the references section

1. **Threat Event Freq**

$$\underline{\mathbf{TEF = COF \times POA}}$$

a. **COF - Contact Frequency (New and improved)**
Assumption: we're limiting to the 3 most likely methods

1. Malvertising (Jansen, 2023)
   10,000 web access a day
   0.021% of all web accesses are phishing in 2022
   2.1 a day
   767 a year

2. Social Engineering (assuming phone calls)
   350 calls a year (Raza, 2023)
   17% are successful
   59.5 contacts a year

3. Software/web Vulnerabilities (2023 Data Breach Investigations Report, n.d.)
   500 software and web vulnerabilities a year
   10% vulnerabilities are exploited
   50 vulnerabilities a year

COF = Email + Malvertising + Social Engineering
COF = 767+59.5+50 attempts per year
COF = 876.5 per year

-/+ 10%
Min = 788.9
Max = 964.1

B. POA - Probability of Action

Estimates *(could not find anything to help support this but aligns with Jack Jones FAIR Institute's Data Integration Workgroup monthly call-in covering ransomware risk to a hospitales)*

1. 40% chance a crime group will exploit Placebo Inc in the next year
2. 25% chance that an APT will exploit Placebo Inc in the next year
3. 10% chance a state sponsored group will exploit Placebo Inc in the next year

Calculation:
Probability that each group does not exploit Placebo
Crime group: 1 - 0.40 = 0.60 (or 60%)
APT: 1 - 0.25 = 0.75 (or 75%)
State-sponsored group: 1 - 0.10 = 0.90 (or 90%)

Probability that none of them exploit Placebo
0.60 ×0.75 × 0.90 = 0.378
This is a 33.75% chance that none of the groups exploit Placebo Inc.

POA:
1 − 0.378 = 0.622

62.2% combined probability that at least one of these groups will exploit Placebo Inc. in the next year.

C. Threat Event Frequency
TEF = COF×POA
TEF = 876.5 X 0.622
TEF = 545.183

Assuming a tolerance of 10%

TEF Figures:
Min: 491
Max: 600
Likely: 545

2. Vulnerability

The data points used to derive Threat Capability are based on reports that identify ransomware as the most used attack against healthcare companies. Ransomware comes in many variants and methods for deployment which makes it trivial for less capable cyber criminals to deploy by reusing old ransomware techniques or variants. As the capability of cyber criminals rises, ransomware is customized code, a result of initial network compromise, result of advanced open source intelligence methods, or uses novel methods that abuse the inherent trust in services, signed packages, or network traffic.
The Resistance Strength metric takes into account sound ransomware security practices as recommended by CISA and intelligence reports from Mitre and Verizon. These practices are implemented into our security strategy to protect assets from ransomware. Use of cyber resiliency practices work to curtail losses by allowing operations to continue during an attack.

a. Threat Capability
    i. Minimum, 50%: It is trivial to obtain ransomware and send it over email or a messaging service. Less capable cyber criminals will not successfully deploy ransomware because simple to detect techniques will be used. Ransomware attacks have increased in sophistication and require various actions to be successful.
    ii. Maximum, 90%: Very capable cyber criminals will easily be able to deploy ransomware and use various advanced methods of deployment where some other initial actions must be taken before deploying ransomware.
    iii. Most likely, 75%: This level of capability should have the expertise to circumvent controls but not be as sophisticated. The majority of attacks are estimated to come from this percentile on the Capability Continuum.
b. Resistance Strength
    i. Minimum: 60%
    ii. Most Likely: 85%
    iii. Maximum: 95%
    iv. Several items in place to resist an attack:
        1. Restrict users' permissions to install and run software applications, and apply the principle of "least privilege" to all systems and services. Restricting these privileges may prevent malware from running or limit its capability to spread through a network.
        2. Use application allow listing to allow only approved programs to run on a network.
        3. Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email to prevent email spoofing.
        4. Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
        5. Configure firewalls to block access to known malicious IP addresses.

6. Update software and operating systems with the latest patches. Outdated applications and operating systems are the target of most attacks.
7. Never click on links or open attachments in unsolicited emails.
8. Back up data on a regular basis. Keep it on a separate device and store it offline.

3. Primary Loss

a. Productivity $251 million / day ($142 million/day - $360 million/day)
    i. Employees - estimated 192,500 based on average of Molina at 15,000 and United at 400,000
    ii. Average pay of $35/hour
    iii. Downtime expense total - $32 million per day
        1. $47 million per day for 192,500 employees minus legal team, PR/comms, breach notifications team, and IT team (in total minus $15 million per day)
    iv. Lost revenue - $219 million/day
        1. Dependent on time of year because of open enrollment period; an attack from November 1 - February 1 will cost more;
        2. Revenue - $80billion / year
        3. $328 million / day during open enrollment and $110 million / day not during open enrollment

b. Response - $100,000 (low of 50K, high of 150K, pulled straight from that blog)
    i. $100,000 for IR team
    ii. PR and communications - assumed already in house so subtract from downtime expense
    iii. lawyers - assumed already in house so subtract from downtime expense
    iv. Breach notifications - assumed that ability already in house

c. Replacement - (min 48,125,000 - avg 96,000,000 - max 144,375,000)
    i. Servers - 9625 at cost of $5K to $15K with avg of $10,000 each = $96 million
        1. 1 server per 20 PCs with est 192,500 PCs gives 9625 servers
    ii. Data Backup up and online cost -> minus IT team from downtime expense

d. Competitive Advantage- if the disclosed information provided evidence of incompetence or criminal activity, competitors could, in theory, leverage that to gain advantage. For the most part, however, we can expect competitors to simply sit back and rake in any disaffected customers (falls under reputation loss).
    Assumed $0

4. Secondary Risk

1. Loss exposure due to “Collateral damage”.

    a. Fines: (losses due to regulatory, civil, or contractual fines)
        1. Minimum: 3,200,000
        2. Most Likely: 33,700,000 (average of minimum and Maximum)
        3. Maximum: 64,200,000

    b. Reputation: Losses due to market share reduction, stock price reduction, increased insurance premiums
        1. Minimum: 48,000
        2. Most Likely: 612,000
        3. Maximum: 1,506,000

    Cybersecurity Insurance: Small business starts at $2,500 per million in coverage.

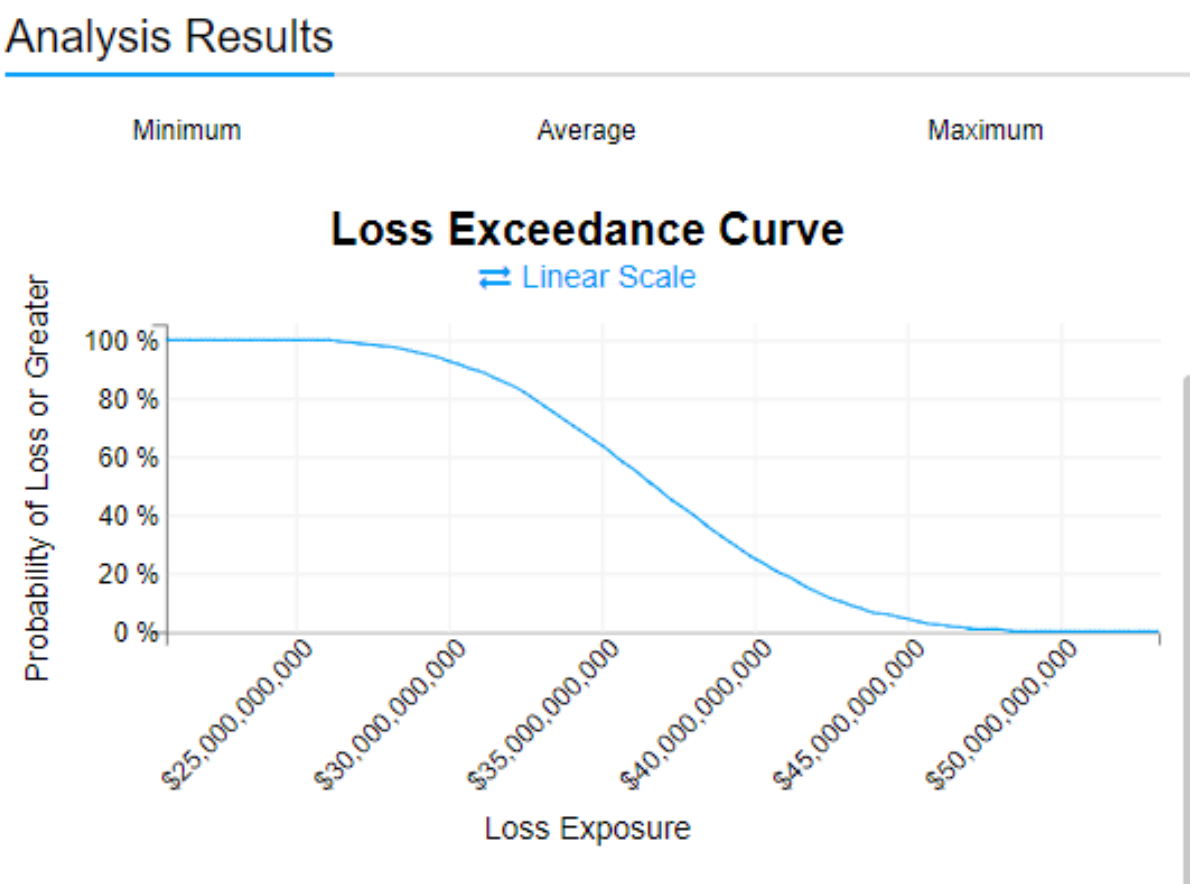
    Assuming medium size business minimum: $10,000/million, Likely: $15,000/million, and maximum: $20,000/million.

    10,000 X 4 = 40,000/year for 4 million in coverage (8000 = 20% increase)
    15,000 X 34 = 510,000/year for 34 million in coverage (102,000 = 20% increase)
    20,000 X 65 = 1,300,000/year for 65 million in coverage (206,000 = 20% increase)

2. Secondary Loss Event Frequency
    Minimum: 95%
    Likely: 97%
    Maximum: 99%

“However, the good news (analytically) when dealing with sensitive customer information scenarios is that you almost always have to engage the customer if their private information has been breached (at least in the United States). This makes SLEF nearly 100%. We say nearly because there can be situations where notification is not required. Consequently, we used a minimum of 95% and a maximum of 100% for the ends of our distribution, and 98% for the most likely value.” (Freund & Jones, 2014, p. 156)

Appendix B - Fair-U Tool



Summary of Simulation Results

Primary

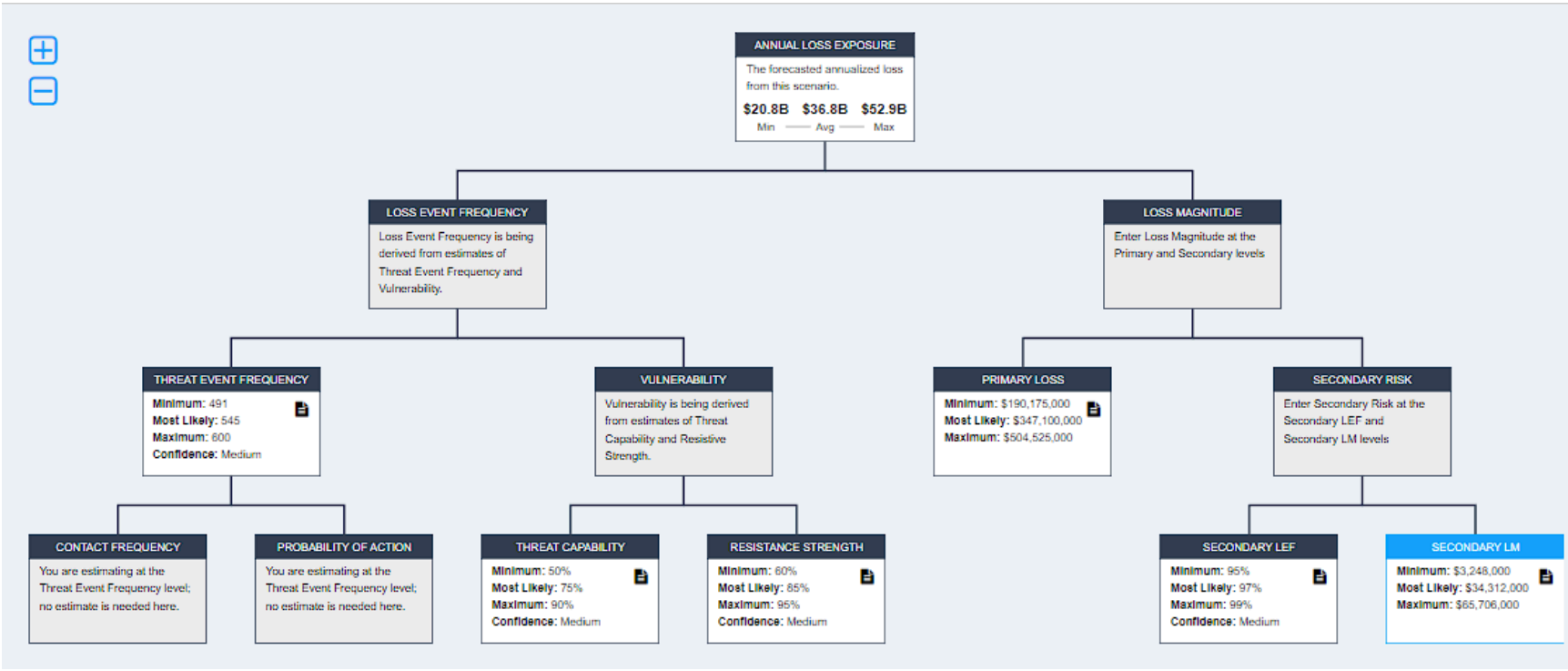
	Min	Avg	Max
Loss Events / Year	87	96.86	107
Loss Magnitude	$210.4M	$346.3M	$481.3M

Secondary

	Min	Avg	Max
Loss Events / Year	80	93.97	105
Loss Magnitude	$5.1M	$34.4M	$64.8M

Vulnerability

17.77%


ANNUAL LOSS EXPOSURE
The forecasted annualized loss from this scenario.
$20.8B $36.8B $52.9B
Min Avg Max
LOSS EVENT FREQUENCY
Loss Event Frequency is being derived from estimates of Threat Event Frequency and Vulnerability.
LOSS MAGNITUDE
Enter Loss Magnitude at the Primary and Secondary levels
THREAT EVENT FREQUENCY
Minimum: 491
Most Likely: 545
Maximum: 600
Confidence: Medium
VULNERABILITY
Vulnerability is being derived from estimates of Threat Capability and Resistive Strength.
PRIMARY LOSS
Minimum: $190,175,000
Most Likely: $347,100,000
Maximum: $504,525,000
SECONDARY RISK
Enter Secondary Risk at the Secondary LEF and Secondary LM levels
CONTACT FREQUENCY
You are estimating at the Threat Event Frequency level; no estimate is needed here.
PROBABILITY OF ACTION
You are estimating at the Threat Event Frequency level; no estimate is needed here.
THREAT CAPABILITY
Minimum: 50%
Most Likely: 75%
Maximum: 90%
Confidence: Medium
RESISTANCE STRENGTH
Minimum: 60%
Most Likely: 85%
Maximum: 95%
Confidence: Medium
SECONDARY LEF
Minimum: 95%
Most Likely: 97%
Maximum: 99%
Confidence: Medium
SECONDARY LM
Minimum: $3,248,000
Most Likely: $34,312,000
Maximum: $65,706,000