Placebo Inc.

Factor Analysis of Information Risk (FAIR) ASSESSMENT

Pelumi Akande | Ross Barber | Carina Martinez-Lopez | Zoe Medina | Randall Seymore

Table of Contents

Executive Summary

Factor Analysis of Information Risk (FAIR) is a risk assessment framework devised to deliver a thorough understanding and quantification of Risk. It offers a structured taxonomy for classifying various components that constitute a risk to information managed by organizations, reinforced by a standard nomenclature to ensure consistency during analysis. Emphasis on using consistent measurement scales for risk factors provides assurance that risks are assessed and interpreted uniformly across various scenarios and by different analysts. The approach is adept at calculating risk with accuracy, offering a tangible value associated with potential risk events. Lastly, it is important to highlight that FAIR integrates both quantitative and qualitative analysis approaches. This hybrid methodology allows risk values to be numerically quantified for precise assessments while remaining understood in terms of contextual significance.

A FAIR analysis was conducted for Placebo, Inc. to provide a better understanding of potential risks from ransomware attacks. This risk stems from the calculated Vulnerability value of the company’s electronic health records system combined with the increasing capabilities of cyber threat actors.

Analysis

Stage 1: Identify scenario components

Asset at Risk

Asset Components from the provided asset list that are likely to be targeted in a ransomware attack are web servers, user and provider data storage, and corporate data. Web servers are likely to be held ransom because it cripples the availability of the service that the company is providing to customers. If customers can no longer reach the website to get information about or purchase the health insurance, the company will lose business and revenue. User and provider data storage is likely to be held ransom because it contains the personally identifiable information and personal health information of customers that are purchasing the health insurance. This is a high value target because attackers can leverage the value of the PII and PHI to get big payouts due to the high fines the company faces if the information is leaked or stolen. Corporate data is likely to be held ransom because it contains personally identifiable information of the employees of the company. Holding this information can also result in big payouts or be sold on the dark web for profit.

Threat Community under Consideration

The threat community most likely responsible for a ransomware attack is organized criminals. These criminals are typically sophisticated in their hacking techniques and have the resources and finances necessary to carry out large scale attacks. In addition, this threat community is typically motivated by financial gain, which is ransomware's primary goal.

Stage 2: Evaluate Loss Event Frequency (LEF)

Threat Event Frequency (TEF)

Given the current trend in ransomware attacks and based on data from other similar organizations:

- Estimated at 1 event every 2 years, or 0.5 events/year?

Threat Capability (TCap)

Considering the expertise and sophistication of ransomware attackers in the present day:

- On a scale of 1-100 (100 being the highest capability), TCap is estimated at 80?

Control Strength (CS)

Review of the average healthcare insurance company’s cybersecurity defenses against ransomware

- Assuming Placebo Inc. has up-to-date anti-malware software, network segmentation, regular backups, and employee training on phishing, CS is estimated at 75?

Derive Vulnerability (Vuln)

Vuln is derived using TCap and CS.

Vuln = TCap - CS

Vuln = 80 - 75

Vuln = 5

Derive Loss Event Frequency (LEF)

LEF is derived using TEF and Vuln.

- If Vuln is 1 (on a scale of 1-10), then the potential of exploitation given a threat event is 10%.

- LEF = TEF * 0.10

= 0.5 * 0.10

= 0.05 events/year.

Stage 3: Evaluate Probable Loss Magnitude (PLM)

Based on Stage 2 we determined that the probability of a total loss event was(XXXXX). We can only hope and set security measures in place to prevent a loss, however, it is important to know the potential outcomes and how to overcome them if a threat attack does occur. Probable Loss Magnitude (PLM) will allow us to determine the overall loss in the event a total loss does occur. Losses are not solely caused by one specific event but can be caused by a variety of factors and small attacks ranging from spoofing and phishing to more malicious intended attacks such as trojans, worms, ransomware, and more.

Worst-Case Loss

Customers, providers, and workers can all play a factor in worst-case loss. The loss of patient trust, potential lawsuits, regulatory fines, and downtime are all points of consideration. Misuse of PHI or a HIPPA violation can cost the company a minimin of $50,000 per case.

- Estimated at $200,000 per year or approximately 4 cases per year.

Probable Loss Magnitude (PLM)

Considering that not every ransomware incident results in the worst-case scenario:

- Assuming 20% of the worst-case loss, PLM = 0.20 * $200,000 = PLM $40,000

Stage 4: Derive and articulate risk

Risk

Upon calculation of the Probable Loss Magnitude in Stage 3, the risk can now be delineated in terms of a monetary value by multiplying the PLM by the Loss Event Frequency. The product of this calculation represents the probable quantitative risk Paclebo Inc. can likely expect if an attack were to take place on the company's electronic health records system.

As seen by the calculation below, the LEF of 0.05 events per year, is multiplied by PLM of $40,000 per event. When totaled, Placebo Inc.'s overall average annualized loss, or Risk, comes out to $20,000 per year.

- Risk = LEF * PLM

- Risk = 0.05 events/year * $40,000/event = $2,000/year.

Recommended Actions

Placebo, Inc. faces a potential risk of a ransomware attack leading to an average annualized loss of $20,000. This risk arises primarily from the vulnerability of electronic health records, the increasing sophistication of threat actors, and the consequent potential financial and reputational impact of such an event. Regular review and enhancement of control measures are highly recommended to mitigate this risk.

Based on the analysis conducted for Placebo, Inc. concerning the risk due to ransomware, here are the recommended actions for managing this risk:

1. Enhance Cybersecurity Controls:

Strengthen existing cybersecurity controls to reduce vulnerability. This includes implementing and continuously updating anti-malware software, network segmentation, regular data backups, and conducting employee training on phishing awareness. Ensure that security measures leverage robust authentication mechanisms and prioritize staff training to minimize the likelihood of breaches.

2. Invest in Threat Intelligence and Detection:

Invest in threat intelligence solutions and advanced threat detection mechanisms. These technologies can help in identifying potential ransomware threats at an early stage, allowing for a proactive response to mitigate the impact.

3. Develop an Incident Response Plan:

Develop and regularly test an incident response plan specific to ransomware attacks. This plan should include clear procedures for isolating affected systems, notifying stakeholders, and engaging with law enforcement if necessary. It should also outline steps for recovery and business continuity.

4. Data Encryption and Backup Strategy:

Implement strong data encryption practices to protect sensitive information from being accessed in the event of a breach. Ensure that data backups are regularly performed and stored securely, so that data can be restored if it is compromised.

5. Regularly Update Security Policies:

Continuously review and update security policies and procedures to adapt to evolving ransomware threats and industry best practices. These policies should be communicated effectively to all employees.

6. Cybersecurity Training and Awareness:

Invest in ongoing cybersecurity training and awareness programs for employees at all levels within the organization. Employees should be educated on the latest ransomware tactics and how to identify and report potential threats.

7. Incident Simulation Exercises:

Conduct periodic ransomware incident simulation exercises to test the effectiveness of the incident response plan and the readiness of the organization to handle a real ransomware attack.

8. Evaluate Cyber Insurance:

Consider purchasing cyber insurance coverage tailored to ransomware events. This can help mitigate financial losses in the event of a successful ransomware attack.

9. Collaboration with Industry Groups:

Collaborate with industry groups and information-sharing organizations to stay updated on the latest ransomware threats and best practices for mitigation.

10. Regular Risk Assessment Updates:

Periodically review and update the risk assessment, taking into account changes in the threat landscape, new vulnerabilities, and the effectiveness of implemented controls.

These recommended actions aim to reduce the risk associated with ransomware attacks and enhance the organization's resilience. By proactively addressing potential vulnerabilities and having a robust incident response plan in place, Placebo, Inc. can better protect its assets and sensitive data while minimizing the potential financial impact of ransomware incidents.

Glossary

Factor Analysis of Information Risk (FAIR)

Ransomware

Electronic Health Records (EHR) System

Personally Identifiable Information (PII)

Loss Event Frequency (LEF)

Threat Event Frequency (TEF)

Threat Capability (TCap)

Control Strength (CS)

Vulnerability

Risk

References