AUJAS CYBERSECURITY

NSE NSEIT

Introduction to Information Security Risk Assessment using FAIR (Factor Analysis of Information Risk)

Author:

Anand Nair,

Principal Consultant - Risk Advisory

AUJAS
CYBERSECURITY

Table of Contents

Executive Summary.....3

- Introduction to FAIR.....4
- Components of the risk landscape.....4

FAIR Risk Assessment.....5

- Risk.....5
- Controls.....5

FAIR Approach.....6

- Stage 1 – Identify scenario components.....7
- Stage 2 – Evaluate Loss Event Frequency (LEF).....8
- Stage 3 – Evaluate Probable Loss Magnitude (PLM).....10
- Stage 4 – Derive and articulate Risk.....12

Conclusion.....13

United States:
Tel: +1 408 973 7205

Middle East:
Tel: +971 6 5528438

India:
Tel: +91-80-2608 7878

contact@aujas.com

www.aujas.com

Executive Summary

Due to the very nature of the world we live and operate, all organizations, be it large corporates or start-ups, are inherently exposed to various information security risks which could potentially disrupt business operations, leading to significant loss of revenue, reputation and probable legal/regulatory actions.

The best way of adopting a cybersecurity framework for organizations is to have a good understanding of what risks are and how they can impact business operations. Organizations should also figure out the probability of these risks occurring given the complex environments they operate; this will arm decision-makers with actionable intelligence and help them make informed decisions.

This paper introduces FAIR (Factor Analysis of Information Risk) model on assessing and understanding security risks. FAIR gives a clear understanding of risks by classifying risk factors and how these factors impact each other to find the probability and frequency of loss events.

Introduction to FAIR

FAIR (Factor Analysis of Information Risk) is a model that codifies a taxonomy of factors contributing to risk and how they affect each other by establishing accurate probabilities for the frequency and magnitude of loss events.

FAIR is a risk analysis framework that organizations can use to translate the impact of cyber risk into financial terms and prioritize risk treatments. It is also a risk assessment model that can objectively quantify the economic consequence of information risks.

Components of Risk Landscape

Before detailing out a risk assessment approach or strategy, let's understand the various components that constitute the risk landscape.

FAIR framework contains four primary components:

1. Threats
2. Assets
3. Organization
4. External environment

FAIR Risk Assessment

The first step in the FAIR approach to risk management is to define and develop a taxonomy for information risk by breaking it down to fundamental components. This approach provides a strong foundation for risk analysis and a useful way to explain analysis results.

Risk: Risk is the probable frequency and probable magnitude of future loss.

The two main components for calculating the risk are **Loss Event Frequency (LEF) and Probable Loss Magnitude (PLM).**

Loss Event Frequency (LEF): LEF is the probable frequency, within a given timeframe, a threat agent can inflict harm on an asset. For a loss event to occur, a threat agent has to act against an asset, and that action must result in a loss.

We can determine this by factoring the **Threat Event Frequency (TEF) and Vulnerability.**

Threat Event Frequency (TEF): The probable frequency, within a given timeframe, a threat agent can act against an asset.

The factors driving threat event frequency are **(a) Contact (b) Action.**

Vulnerability: The probability of an asset's inability to resist the actions of a threat agent. A vulnerability exists when there is a difference between the force applied by the threat agent and an asset's ability to resist that force.

Two primary factors that drive vulnerability are **(a) Threat Capability (b) Control Strength.**

Probable Loss Magnitude (PLM): There are various factors that drive Probable Loss Magnitude. PLM is the potential financial value lost to the organization due to materialization of a risk or loss event.

Controls: A control is a countermeasure or safeguards to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems or other assets. Controls can take one of the three forms – policy, process, technology.

As per FAIR all controls fall into categories. The three primary control categories are:

1. Loss Event Controls
2. Threat Event Controls
3. Vulnerability Controls

FAIR Approach

A simplified risk assessment approach utilizing FAIR is comprised of ten steps in four stages as outlined below:

Stage 1: Identify scenario components

- Identify the asset at risk
- Identify the threat community under consideration

Stage 2: Evaluate Loss Event Frequency (LEF)

- Estimate the probable Threat Event Frequency (TEF)
- Estimate the Threat Capability (TCap)
- Estimate Control Strength (CS)
- Derive Vulnerability (Vuln)
- Derive Loss Event Frequency (LEF)

Stage 3: Evaluate Probable Loss Magnitude (PLM)

- Estimate worst-case loss
- Estimate probable loss

Stage 4: Derive and articulate risk

- Derive and articulate risk

Stage 1: Identify Scenario Components

Identify the Asset at Risk: The first step is to identify the asset at risk and would entail finding out where liability exists. For this example, we will take access credentials to an HR system as the asset which we are evaluating for risks.

Identify the Threat Community: The second step is to figure out the risk associated with the respective threat. At this stage, the assessor should ascertain the potential threats and threat communities, keeping in mind the business of the organization. For this example, our threat community is going to be facilities management personnel.

Stage 2: Evaluate Loss Event Frequency (LEF)

Accepting the fact that the facilities management team comprises of honest people with few skills and knowledge in operating IT systems, the HR system credentials typically would not be viewed or recognized as a valuable item and the perceived risk associated with illicit use by them would be considered low as per the TEF table below.

Rating	✓	Description
Very High (VH)		>100 times per year
High (H)		Between 10 and 100 times per year
Moderate (M)		Between 1 and 10 times per year
Low (L)	✓	Between 0.1 and 1 times per year
Very Low (VL)		<.1 times per year (less than once every ten years)

Estimate the Threat Capability (TCap)

TCap refers to the threat agent's skill and resources which can be used to carry out a successful attack against an asset. It is reasonable to rate the facilities management cleaning personnel TCap as Medium, as compared to the overall threat population.

Rating	✓	Description
Very High (VH)		Top 2% when compared against the overall threat population
High (H)		Top 16% when compared against the overall threat population
Moderate (M)		Average skill and resources (between bottom 16% and top 16%)
Low (L)	✓	Bottom 16% when compared against the overall threat population
Very Low (VL)		Bottom 2% when compared against the overall threat population

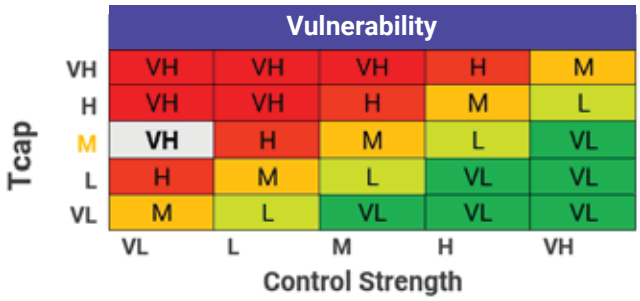
Estimate the Control Strength (CS)

Control Strength is the asset's ability to resist compromise. In use case example below, the credentials are in plain sight and plain text, the CS is consequently "Very low."

Rating	✓	Description
Very High (VH)		Protects against all but the top 2% of an average threat population
High (H)		Protects against all but the top 16% of an average threat population
Moderate (M)		Protects against the average threat agent
Low (L)	✓	Only protects against the bottom 16% of an avg. threat population
Very Low (VL)		Only protects against the bottom 2% of an avg. threat population

Derive Vulnerability (Vuln)

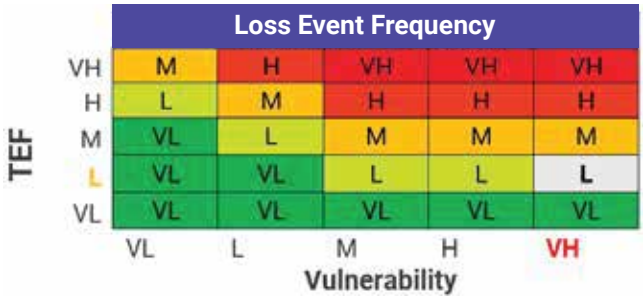
It is easy to derive vulnerability by establishing TCap and CS. The following matrix is used to determine vulnerability.



From the above matrix, we can determine the vulnerability rating by finding out where TCap intersects with the Control Strength. In this case, the vulnerability rating is Very High (VH).

Derive Loss Event Frequency (LEF)

LEF is derived by intersecting Threat Event Frequency (TEF) and Vulnerability within the matrix below.



In our scenario, given a TEF of **"Low"** and the derived vulnerability rating of **"VH"**, the LEF is **"Low"**.

Stage 3 – Evaluate probable Loss Magnitude (PLM)

As per our assessment above, we have determined that the probability of a loss event in our scenario is Low (somewhere between 0.1 and 1 times per year). The next step is to analyze the loss if an event does occur.

Estimate Worst-Case Scenario

In this scenario, three potential threat actions stand out as having significant loss potential – misuse, disclosure, and destruction.

The next step is to estimate the worst-case loss magnitude for each loss form. For this scenario, we'll select "Disclosure" as our worst-case scenario.

	Loss Forms					
Threat Actions	**Productivity**	**Response**	**Replacement**	**Fine /Judgements**	**Comp. Adv.**	**Reputation**
Access						
Misuse						
Disclosure	**H**	**H**	-	**SV**	**H**	**SV**
Modification						
Deny Access						

Magnitude	Range Low End	Range High End
Severe (SV)	$10,000,000	-
High (H)	$1,000,000	$9,999,999
Significant (Sg)	$100,000	$999,999
Moderate (M)	$10,000	$99,999
Low (L)	$1000	$9,999
Very Low (VL)	$0	$999

In the table above, we have not estimated the loss magnitude for "Replacement" since we already have "Fine/Judgements" and "Reputation" as Severe (SV).

Estimate Probable Loss Magnitude (PLM)

To estimate PLM, we should first determine the occurrence of the most likely threat action. In our sample scenario, we are going to surmise the threat agent's primary motivation would be financial gain. In this scenario, for our analysis, given the type of asset (personal information), and the available threat actions, it's reasonable to select "Misuse" as the most likely action – Example, Identity Theft. The next step is to estimate the most likely loss magnitude resulting from Misuse for each loss form.

	Loss Forms					
Threat Actions	**Productivity**	**Response**	**Replacement**	**Fine /Judgements**	**Comp. Adv.**	**Reputation**
Access						
Misuse	M	M	VL	VL	VL	VL
Disclosure						
Modification						
Deny Access						

Magnitude	Range Low End	Range High End
Severe (SV)	$10,000,000	-
High (H)	$1,000,000	$9,999,999
Significant (Sg)	$100,000	$999,999
Moderate (M)	$10,000	$99,999
Low (L)	$1000	$9,999
Very Low (VL)	$0	$999

The rationale for these estimates includes:

- The impact of productivity will be moderate as employees react to the event.
- The cost of responding to the event will include investigation, some amount of time from the legal department and providing compensation to any affected employees.
- Replacement cost would only entail changing the HR system's password.

Stage 4 – Derive and Articulate Risk

Risk is derived from Loss Event Frequency (LEF) and Probable Loss Magnitude (PLM).

PLM \ LEF	VL	L	M	H	VH
	RISK				
Severe	H	H	C	C	C
High	M	H	H	C	C
Significant	M	M	H	H	C
Moderate	L	M	M	H	H
Low	L	L	M	M	M
Very Low	L	L	M	M	M

LEGEND

Key	Risk Level
C	Critical
H	High
M	Medium
L	Low

The next step is to decide whether to articulate the risk qualitatively using the matrix above or to articulate risk as LEF, PLM, and worst-case.

In our scenario, we'll do both.

Using the above matrix, we can report the risk associated with this threat community is **"Medium"** based on the **"Low"** LEF (between 0.1 and 1 times per year) and a **"Moderate"** PLM (between $10,000 and $ 100,000). Additionally, we can also communicate to the decision-maker that worst-case loss could be severe, but the probability of a worst-case outcome is very low.

Conclusion

Driving information security risk assessment in an organization has its challenges. The assessment must align with the enterprise risk framework and should be able to articulate the risk in a way senior leadership of business decision-makers can clearly understand and appreciate. This challenge exists owing to the very nature of information flow within an organization and the myriad ways it can be compromised.

While there are many approaches to carrying out information security risk assessments in an organization, it is still challenging to accurately reflect the true nature of risks.

FAIR seeks to provide a practical and logical foundation through its taxonomy, definitions, and analysis methods. The benefits include:

1. Clearer, consistent, and better quality of risk analysis.
2. Provides confidence to risk assessors to conduct analysis in a logical fashion.
3. Boosts confidence among senior leadership/business decision-makers.
4. Significant improvement in the ability to cost-effectively manage risks.

About Aujas

Aujas cybersecurity is an enterprise security service provider for organizations across North America, Asia Pacific, and EMEA regions. Aujas has deep expertise and capabilities in Identity and Access Management, Risk Advisory, Security Verification, Security Engineering & Managed Detection and Response services. By leveraging innovative products and services, Aujas helps businesses build and transform security postures to mitigate risks. The service focus is to strengthen security resilience by minimizing the occurrence of sophisticated attacks and threats while offering 360-degree visibility and protection across enterprise infrastructure.

For more information, do visit us at **www.aujas.com**

You can also write to us at **contact@aujas.com**