University of Cincinnati

Date: 2/17/2020

I, Adeyinka A. Bakare, hereby submit this original work as part of the requirements for the degree of Master of Science in Information Technology.

It is entitled:

A Methodology for Cyberthreat ranking: Incorporating the NIST Cybersecurity Framework into FAIR Model

Student's name: **Adeyinka A. Bakare**

This work and its defense approved by:

Committee chair: Hazem Said, Ph.D.

Committee member: Bilal Gonen, Ph.D.

UNIVERSITY OF Cincinnati

36567

A Methodology for Cyberthreat ranking: Incorporating the NIST Cybersecurity Framework into FAIR Model

A thesis submitted to the

Graduate school

of the University of Cincinnati

in partial fulfillment of the

requirements for the degree of

Master of Science

in the School of Information Technology

of the College of Education, Criminal Justice, and Human Services

by

Adeyinka A. Bakare

Bachelor of Science – Information and Communication Science

University of Ilorin, Nigeria.

March 2020

Committee Chair: Dr Hazem Said

Committee Member: Dr Bilal Gonen

ABSTRACT

The National Institute of Standards and Technology (NIST) recommends that organizations perform cyber risk assessments regularly to identify security vulnerabilities and to control levels of exposure to threats (Barrett, 2018). The implementation of the NIST Cybersecurity Framework (CSF) is a model to identify an organization's current security strength level, compliance gaps, and deficiencies (NIST, 2014b). To comply with the CSF, NIST recommends security controls for Federal Systems and Organizations (NIST, 2014b). Measuring an organization's compliance with these controls enables the organization to direct its resources towards its cybersecurity infrastructure and to implement a risk mitigation strategy effectively. This thesis discusses a method to rank cyber threats relevant to an organization's readiness, as indicated by its maturity level of implementing NIST CSF controls.

The Loss Event Frequency (LEF), as described by the Factor Analysis of Information Risk framework (FAIR), is the probable frequency in a time range that a cyber threat will inflict harm on an organization's assets to cause a loss. This thesis follows the work of Le et al. (2018) in using the value of the LEF as a measure of the severity of cyber threats. The proposed work uses an organization's maturity level towards the implementation of NIST CSF controls as a replacement of expert opinion in defining the organization's resistance strength to a cyber threat. The use of the maturity level scores provides a direct and more accurate representation of the resistance strength of the organization. The methodology integrates the NIST CSF maturity levels to calculate the resistance strength component and produce the LEF values for threat events; the LEF values represent the severity level of each threat event to the organization and is used to rank Cyber threats. This hybrid risk analysis approach will help an organization make data-informed decisions on improving cybersecurity measures.

Copyright Notice

ACKNOWLEDGMENTS

I would like to thank my advisor, Dr. Hazem Said for his expert advice, encouragement, guidance and support throughout all stages of this thesis work.

I am thankful and grateful to my family and friends for the continuous support and prayers they send my way.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

SECTION 1: INTRODUCTION

1.1 Background

Cyberthreats continue to impact business continuity and pose a risk to organizations (Ponemon Institute, 2018). In Kaspersky Lab (2015), the Global IT Risks Survey showed that 50% of the respondents ranked cyber threats as a leading business threat, next to economic uncertainty. A recent survey, Marsh Microsoft (2019) reported that "79% of respondents ranked cyber threats as the top concern than any other major business risk, a full 20 percentage points above Economic uncertainty". The sharp rise in the prominence of cyber threats in recent years shows that cyber threats have become the next top business risk. Due to this evolution, identifying threat events remain crucial to the risk assessment process (Alali et al., 2019). Le et al. (2018) advised that the ranking of cyber threats will help managers make better decisions regarding security countermeasures and mitigation plans. Krishan (2018) reported that the average cost of a security breach in an organization in the United States is about $6.4 million, resulting in $225 per compromised record. Most of these attacks target confidential and financial information or intellectual properties of the organization.

Multiple studies (Alali et al., 2018; Aven, 2015; Barrett, 2018; Cherdantseva et al., 2016; Clark et al., 2004; Farahmand et al., 2005; Figueira, Bravo & Lopez, 2020; Fenz, 2014; Gabriel, Shi, & Ozansoy, 2017; Ibrahim et al., 2018; Le et al., 2018; Wang, Neil & Fenton, 2019) agreed that cybersecurity risk assessment plays a crucial role as a preventive measure in the information security system of any organization. By performing a comprehensive cyber risk assessment, an organization understands its current cybersecurity risk level and can move forward to take sophisticated and prioritized steps to reduce such risks (National Institute of Standards and Technology, 2012). Recognition of the severity of cyber threats prompted a former President of The United States to sign an Executive Order (Executive Order 13636, 2013), directing government agencies to develop models to improve cybersecurity risk management processes in the country.

The National Institute of Standards and Technology (NIST), a US Government agency, developed the Cybersecurity Framework (CSF), a cybersecurity risk assessment framework used by public and private organizations that own, operate, or supply critical infrastructure (NIST, 2014b). This framework provides basic processes and essential controls for cybersecurity, which are used for a cyber risk quantitative assessment to determine the current state of a system (Barrett, 2018, NIST, 2014b). The CSF allows an organization to highlight the cybersecurity weakness and strength of its policies. A survey of IT security professionals in the United States revealed that 70% of organizations view NIST's CSF as a security best practice (Dimensional Research, 2016). However, Jones (2016) pointed out that the major limitation of NIST CSF is the lack of an analytic capability that would allow its users to quantify cyber risks as well as the probable cost of non-compliance gaps in their organizations.

One framework that compensates for this limitation is the Factor Analysis of Information Risk (FAIR) model. The FAIR model is an analytic model that enables quantitative measurement of an organization's cyber risk (Freund & Jones, 2015). FAIR provides a model for analyzing, quantifying, and understanding cyber risk in financial terms. It utilizes a hierarchical structure made up of two major components, Loss Event Frequency (LEF) and Loss Magnitude (LM) to measure risk. The LEF represents a measure of the relationship between the strength of a threat event and the strength of an organization in defending against the threat. If a threat event is sophisticated, happens frequently, and the organization's defense is strong, the LEF will have a low value. However, if the threat levels are high and the organization's defense is weak, the LEF will be a high value. To prove the validity of FAIR's compatibility with NIST CSF, NIST officially published FAIR as an Informative reference to its CSF standard (NIST, 2019). This shows that there is a direct mapping between FAIR and CSF in the categories covering risk analysis and risk management. FAIR Institute Blog, (2019) announced that "This is confirmation that organizations can be confident employing FAIR for their risk analyses alongside the other NIST CSF framework processes."

1.2 Purpose of Study

This thesis introduces a hybrid cybersecurity risk analysis approach to rank cyber threats based on the current state of an organization's system. The proposed method incorporates an organization's NIST CSF maturity values into the FAIR model to quantitatively rank cyberthreats. I used the threat-to-mitigation index mapping table available in Vasenev et al. (2015), to integrate an organization's control values as resistance strength in the LEF computation. The aim of this work is to help stakeholders make data-informed decisions on improving security measures based on threat severity and provide accurate values that represent the current state of their system. The proposed method will improve the risk analysis process by identifying threat events with the highest severity based on the current state of an organization, thereby reducing dependence on expert opinions that tend to be inconsistent and inaccurate depending on their level of experience.

SECTION 2: LITERATURE REVIEW

The literature review includes four areas of focus: (a) cybersecurity threats and risks (b) cyber risk frameworks (c) qualitative, quantitative and hybrid assessment of cyber risk, and (d) threat ranking based on quantitative assessment.

2.1 Cybersecurity threats and risks

Over the years, organizations have experienced a considerable rise in the sophistication of cyber-attacks. American corporations are greatly affected by this because it takes an average of 46 days to resolve a cyber-attack or security breach, which results in $21,155 loss per day (Krishan, 2018). These costs present a huge liability to organizations, and it can escalate into more disastrous consequences such as disruption of services, competitor advantage, and legal repercussions (Ponemon Institute, 2018). To reduce these risks, some studies (Alali et al., 2018; Cherdantseva et al., 2016) prescribed the urgent need to develop a specialized cybersecurity risk assessment model that will help to identify and mitigate risk, and it may also help prevent losses due to the continuous cyber threats.

Multiple studies (Aven, 2015; Cherdantseva et al., 2016; Clark et al., 2004; Fenz et al., 2014; Gabriel et al., 2017; Hiller & Russell, 2017) focused on reviewing the pros and cons of several cybersecurity risk frameworks concerning their ability to mitigate risks and strengthen a security system against threats. A few studies (Gabriel et al., 2017; Hiller & Russell, 2017; Ibrahim et al., 2018), proposed that an integrated framework will provide the most economic advantage to an organization, and Krishan (2018) recommended the creation of a specialized risk analysis system and incident support teams to tackle cyber threats.

2.2 Cyber Risk Frameworks

Measuring how efficient and effective cybersecurity frameworks are towards managing real-life cyber risks is crucial to understanding its economic impact on any organization (Wheeler, 2011).

Organizations are required to take a systematic approach when implementing a risk management framework (Hiller & Russell, 2017). Some studies (Fenz et al., 2015; Ibrahim et al., 2018), investigated the top cyber risk frameworks available and described their effectiveness and challenges. The cybersecurity frameworks investigated were: NIST SP 800-53 Rev. 4. (NIST, 2014a); NIST CSF version 1.0 (NIST, 2014b); Control Objectives for Information and Related Technologies - COBIT5, (ISACA, 2012); ISO/IEC 27001:2013 - published by International Organization for Standardization and the International Electrotechnical Commission (ISO, 2013); International Society of Automation (ISA) 62443-2-1:2009 (ISA, 2009); and ISA 62443-3-3:2013 (ISA, 2012). Ibrahim et al. (2018) provided a case study with examples of their implementations and declared that NIST CSF offers the most advantage by leveraging and integrating the major features of other frameworks.

Ibrahim et al. (2018) stated that NIST CSF is one of the top preferred frameworks used by organizations because its structure was designed to evolve with changes in cybersecurity threats, processes, and technologies. These organizations usually develop their custom assessment tools based on the NIST CSF model, because of its ease of use and flexibility in targeting individual areas of an organization to measure the risk level. The primary function of such a tool is to determine the level of security compliance of any unit in the organization, and it can also evaluate the organization's system to identify the risks/possible threat areas.

2.3 Qualitative Assessment

In practice, a qualitative risk assessment is a process of using ordinal rating scales (e.g., green-yellow-red, low-medium-high) to determine risks based on their likelihood of occurrence and impact of loss to the organization. Going by this, organizations can visually represent the relative severity of the various risks the organization faces. One major downfall of this type of approach is that the range of values

in a qualitative assessment is usually small, this makes different experts rely on their personal experiences to produce meaningful but inconsistent results from them (NIST, 2012).

Qualitative risk assessment is efficient, useful in making quick decisions, and easy to communicate. However, the downsides associated with this approach are bias and inconsistencies in risk assessment results, as well as ambiguity in meaning (what does "red/high" really mean?). Another issue lies with risk prioritization and mitigation. When there are multiple red risks, how does an analyst decide which to mitigate first? Which one is "reddest"? Succinctly, the qualitative approach presents a systematic analysis that provides ordinal results rather than a numerical result (Clark et al., 2004). Although the results are reliable, in many cases, the ordinal results are not detailed enough to make clear decisions (Ibrahim et al., 2018).

2.4 Quantitative Assessment

Alali et al. (2018), states that quantitative assessment depends on probabilistic and statistical approaches towards an uncertain event. Quantitative risk assessment minimizes the tendency towards bias and inconsistencies if integrated with a well-defined model to evaluate risk. Moreover, it addresses the prioritization problem by utilizing economic terms (e.g., dollars and cents) as its measurement, rather than an ordinal or relative scale. Clark et al. (2004), confirmed that the quantitative method enhances analysis by scoring the effectiveness of current and potential security solutions. The objective of the quantitative assessment is to utilize probability theory and statistics to assign probabilistic numerical values to threat likelihood (Farahmand et al., 2005). Although this method provides clear guidance about the threat, it usually has a high level of difficulty in implementation and ambiguity evaluation (Fenz et al., 2014).

One of the most popular frameworks for the quantitative cyber risk assessment is the Factor Analysis of Information Risk (FAIR) model (Wang, Neil & Fenton, 2019). FAIR's definition of risk is related

to the same in Aven (2015), which states that “Risk is the possibility of an unfortunate occurrence.” The FAIR model ensures that the same rigorous and consistent approach is maintained across an analysis; this allows accurate comparison of data.

2.5 Hybrid Assessment

Multiple studies (Alali et al., 2018; Figueira et al., 2020; Gabriel et al., 2017; Le et al., 2018) attempted to create a hybrid approach by integrating their own algorithm/models into a framework. Alali (2018) proposed a fuzzy inference modeling method based on four risk factors, and the process extended the NIST framework to specify the range of risks that can threaten a system. Gabriel et al. (2017) proposed a method to align the NIST framework with a Funnel Risk Graph Method (FRGM) approach, and the authors expect the recommended process to minimize or eliminate loss to an organization. Figueira et al. (2020) extended the ISO framework (ISO, 2013) by incorporating threat-occurrence predictive models in a bid to create a hybrid cyber risk analysis approach, the authors focused on predicting the future occurrence of threat and not an organization’s ability to resist those threats. Le et al. (2018) presented a method to integrate the FAIR model’s structural analysis into a Bayesian Network system to obtain the LEF numerical threat assessment which helps identify the most influential factor to improve the mitigation effectiveness, and the risk managers can then formulate a more effective mitigation plan, which includes the most cost-effective security countermeasures to lower the threats’ impacts.

The multiple approaches to risk assessment can make it difficult for a new organization to determine which will be useful. NIST (2012) mentioned that risk assessment approaches used by organizations are dependent on the culture and attitude of the organization towards risk events. The three methods that determine how an organization handle risks as presented in NIST (2012) are:

i. Threat-oriented: this focuses on initially identifying threat sources, events, and development of threat scenarios, the next step is identifying vulnerabilities in the context of the threat, and finally, impacts are determined based on adversary intent.

ii. Asset/impact-oriented: this starts with the identification of impact levels or consequences of critical assets, and then identification of threat events/sources that could cause those impacts or consequences

iii. Vulnerability-oriented: this starts with a set of exploitable weaknesses in an organizational information system and then identifies the threat events that could exploit such vulnerabilities and their probable impact/consequences.

The three methods above use the same risk factors and contain the same set of activities during a risk assessment. NIST (2012) concluded that the difference in starting points could help improve the effectiveness of a cyber risk analysis.

2.6 Threat Ranking

Le et al. (2018) proposed a method to rank cyber threats by extending FAIR's functionality of obtaining the LEF value. The author incorporated the FAIR model into Bayesian Network to reconstruct a continuum of LEF values, which helped to improve the assessment of multiple threat events in the same category, and the method made threat ranking easily achievable and reliable. NIST (2012) outlined a comprehensive list of 102 possible threats events, and Vasenev et al. (2015) refined the list to 32 potential smart-grid related threats, Le et al. (2018) focused on the first 14 out of the 38 IRENE (Improving the Robustness of Urban Electricity Networks) threat events outlined in Vasenev et al. (2015), and successfully ranked the threat based on the numerical assessment (LEF) values derived. Although some of the threat events in the same category had fuzzy input values used for the evaluation in the FAIR model, the incorporation of the Bayesian Network model helped produce a more granular assessment value, which made the ranking of those threats possible.

SECTION 3: RESEARCH STATEMENT

Based on the review of related literature I discovered that there is a growing need for a real hybrid assessment framework that incorporates both qualitative and quantitative approaches, ranking of cyber threats enables organizations to identify cyber threats with the highest severity make faster decision in prioritizing their efforts in improving security posture, and there is currently no method available to rank cyber threats based on the current state of an organization. Despite both the NIST CSF and FAIR model being one of the most accepted and popular qualitative and quantitative frameworks, respectively, no researcher has moved to incorporate them together to form a hybrid assessment approach. This led to the formulation of my hypothesis.

3.1 Hypothesis

I hypothesized that "Integrating NIST CSF and FAIR to form a hybrid risk assessment approach will create a pragmatic cyber threat ranking based on the actual security posture of an organization."

3.2 Value Proposition

To test my hypothesis, I defined the following propositions in this research:

- Create a hybrid assessment method that can quantify the severity of threat events in an organization.
- Integrate an organization's security posture into the resistance strength factor required by the FAIR model for a quantitative risk assessment.
- Use FAIR's LEF value to rank threats in order of the severity of their impact on the organization.

The remaining sections of this thesis will: describe the methodology in detail, present the application of the method, results, and conclusion of this work.

SECTION 4: METHODOLOGY

This methodology section covers the following areas, (a) Related concepts (b) Incorporating NIST CSF to FAIR model (c) Threat Scenario Simulator Tool, and (d) Applying the method.

4.1 Related Concepts

4.1.1 The NIST Cybersecurity Framework

The National Institute of Standards and Technology Cybersecurity Framework version 1.1 (NIST CSF) consists of best practices, standards, and guidelines to manage cybersecurity program risk (Barrett, 2018). This voluntary, versatile, and flexible framework is divided into three components, Core, Profile, and Tiers. The CSF Tiers are used by an organization's stakeholders to clarify how it views cybersecurity risk and determines the degree of sophistication of its risk management approach. The CSF Profile describes the cybersecurity activities performed by an organization and what outcomes they are achieving based on their needs and risk assessments.

The CSF Core is comprised of five functions which are, Identify, Protect, Detect, Respond, and Recover. The structure of these functions is designed to promote communication between technical experts and business stakeholders in the cybersecurity domain, enabling cyber risk management to merge into the overall risk management strategy for an organization. The CSF Core functions are further broken down into categories and subcategories, and there are currently 23 categories and 108 subcategories alongside informative references that maps each subcategory to other major security frameworks, this enables organizations to review existing controls and policies as well as implement new controls to improve the cybersecurity posture of their organization.

Although the CSF does not prescribe controls explicitly, the subcategories have outcome-driven statements that provide considerations for creating or improving a cybersecurity program. Table 1 summarizes the Framework Core's Functions and Categories.

Table 1: NIST Cybersecurity Framework – Core (Barrett, 2018)

NIST Cybersecurity Framework					
FUNCTIONS	**Identify**	**Protect**	**Detect**	**Respond**	**Recover**
CATEGORIES	Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
	Business Environment	Awareness & Training	Security & Continuous Monitoring	Communications	Improvements
	Governance	Data Security	Detection Procedures	Analysis	Communications
	Risk Assessment	Information Protection, Processes & Procedures		Mitigation	
	Risk Management Strategy	Maintenance		Improvements	
	Supply Chain Risk Management	Protective Technology			

The Cybersecurity Framework's built-in customization mechanisms make it versatile and applicable to organizations of all sizes, sectors, and maturities (Barrett, 2018). Because the Framework is voluntary, outcome-driven, and does not dictate how to achieve those outcomes, it enables customizable risk-based implementations based on the needs of an organization. Readers should refer to NIST CSF Online Learning (n.d.) for examples of how industries and organizations have used the Framework, several use cases, and reasons for using the Framework.

4.1.2 The FAIR Model

The Factor Analysis of Information Risk (FAIR) model is a well-known risk assessment framework (Freund and Jones, 2015) that has been named one of the most popular models for quantitative cyber risk assessment (Wang et al., 2019). The model describes the necessary building blocks in a hierarchical structure for practical implementation in a cyber risk management process. One of the top value propositions of the FAIR framework is its ability to deliver a consistent and reliable model for measuring risk by decomposing it into its core components of frequency and magnitude, which is not present in other

cyber risk frameworks (Fred & Jones, 2015). The FAIR analysis process consists of 5 steps leading to a Risk value: Identifying risk scenarios, FAIR factors, Expert Estimation, PERT (Program Evaluation and Review Technique), and Monte Carlo engine (Fred & Jones, 2015).

This thesis focused on the loss frequency component - LEF, the LEF component is made up of two significant factors, Vulnerability and Threat Event Frequency, these are further broken down to two elements respectively (The Open Group, 2009):

Threat Event Frequency is the occurrence, within a given timeframe, that a threat agent will act against an asset.

- *Contact Frequency (CF)*: probable frequency, within a given timeframe, that a threat agent will encounter an asset.
- *Probability of Action (PA):* the likelihood that a threat agent will act against an asset once contact occurs.

Vulnerability is the probability that an asset will be unable to resist the actions of a threat agent.

- *Threat Capability (TC)*: probable capability a threat agent can apply against an asset.
- *Resistance Strength (RS)*: also referred to as control strength, is the strength of a Control as compared to a baseline measure of force.

The hierarchical structure of the FAIR model is illustrated in Figure 1. Readers should refer to The Open Group (2009) for full details of the FAIR taxonomy.

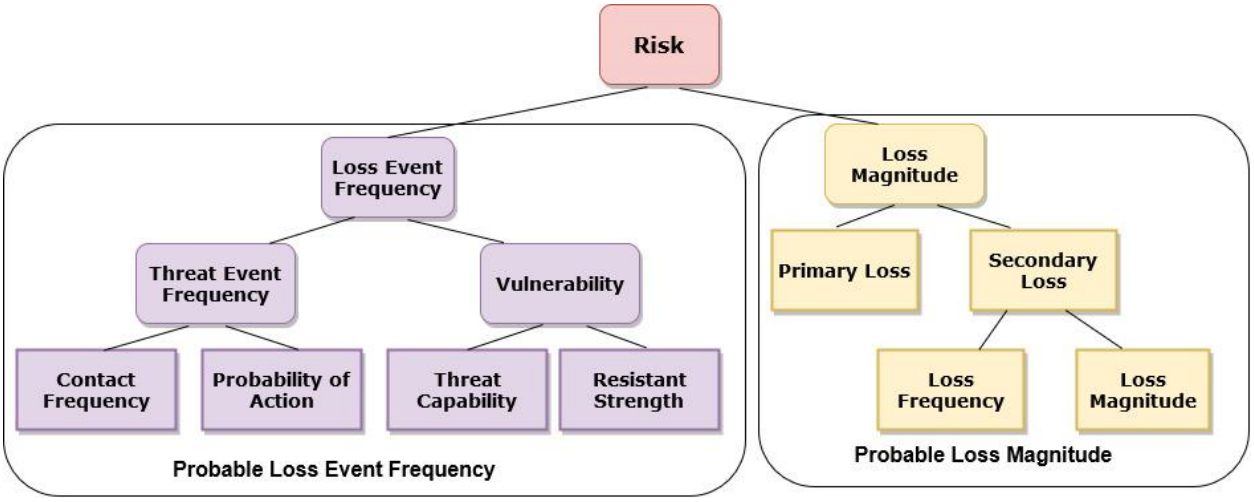

Figure 1: Taxonomy of the FAIR Model.

The latest implementation of the FAIR model found in the official FAIR web analysis engine (FAIR-U, n.d.) allows modeling of inputs for individual threat factors in the form of a percentage range of 0% – 100% spread across three groups (i.e. [Minimum, Most Likely, and Maximum] or [MN, ML, MX]). FAIR expects the inputs to be well-estimated guesses from security experts based on the wealth of experience gained in their field and knowledge of the organizational security environment, which they represent.

Previous implementations of the FAIR model used a five-point scale (i.e. [Very Low, Low, Moderate, High, and Very High] or [VL L M H VH]) such as one used by Le et al. (2018), this made it relatively easier for experts to give their opinions by selecting a value from the ordinal range (VL L M H VH), for each threat factor. Recent implementations of FAIR require quantitative values, which put more pressure on the experts in providing accurate estimates.

A problem we encountered early on was the conversion of qualitative input values of the previous implementations of FAIR to quantitative values required in the latest implementations. NIST (2012) provided a 'qualitative value' – 'semi-quantitative value' assessment scale for threat factors, as shown in Table 2, which remedies the problem.

Table 2: Assessment scale of threat actors (NIST, 2012).

Qualitative Values	**Semi-Quantitative Values**	
Very High	96-100	10
High	80-95	8
Moderate	21-79	5
Low	5-20	2
Very Low	0-4	0

The assessment scale in Table 2 provides the equivalent semi-quantitative values of a threat factor's qualitative value in two forms: a range of values and a single value. The first form, a range of values, can be modified for use as the input model for threat factors in the new implementation of FAIR when performing a conversion with a dataset used in the previous implementation.

Le et al. (2018) developed an innovative use of the FAIR model and integrated it into another model, the Bayesian Network, to rank threats based on their LEF values. In this thesis, I focused on developing a parallel method against the research carried out by Le et al. (2018), thereby using the same set of data as their study. This method incorporates FAIR and NIST CSF 1.1 together to provide a more accurate representation of an organization's readiness to mitigate and resist threats and rank those threats based on their severity (LEF) value.

4.2 Incorporating NIST CSF into the FAIR model

Well-defined frameworks still encounter challenges when analyzing and communicating risk, and this is because Risk is inherently complicated (NIST, 2012). FAIR's significant advantage in this aspect is its ability to provide a greater understanding of the contributing factors to risk. The FAIR's structural framework consists of several pairs of event relations, also known as threat factors, that can lead to an expected loss exposure. This simplified breakdown of factors that constitutes Risk makes it easy for

experts to make consistent and clear assumptions that can lead to effective decisions and recommendations.

According to Barrett (2018), NIST CSF uses the Program Review for Information Security Management Assistance (PRISMA) scale in Bowen and Kissel (2007) to assign a score to each of the implemented controls. The PRISMA scale builds upon the five levels of maturity (i.e., policy, procedures, implementation, test, and integration), which translates to a score range of 1 – 5 for each control in the subcategories of the CSF.

The Information Technology Solutions Center (ITSC) at the University of Cincinnati developed an enterprise-level software application in collaboration with a Fortune 500 company, called Enterprise Security Management (ESM). The ESM application is an organizational risk management system with the practical implementation of the NIST CSF 1.1 framework. It uses the same nested level structure (i.e., Functions, Categories, Subcategories) as the CSF, and helps an organization store and monitor the progress of their implemented controls, calculate maturity values of those controls across different business units, identify compliance gaps and generate reports of the organization's security strength.

Due to the versatile and flexible nature of the CSF, the ESM application was built to tailor the CSF to better align with the organization's business needs. The ESM application modified the framework core component to set more explicit criteria for the measurement of security posture by adding extra layers of granularity to outline the organization's implementation strategy, the extra layers created are:

- Controls: Since the CSF does not explicitly prescribe security controls, this was created as a sub-level of the CSF Subcategories
- Technology, Process & People (TPP) - as a sub-level of controls.

The TPP represents the individual elements that organizations take actions on to improve their security posture, and it also determines the maturity level of the controls. The TPP can be defined as:

- Technology: This is the technical implementation of controls objectives; they usually require money to implement and integrate into the system. (e.g., 2FA, Firewall, Badge readers for doors.)
- Process: This refers to the business goals, policies, and objectives that drive successful changes in a business. (e.g., data center policies, data classification, security policies.)
- People: This represents the users of the system; they utilize the technologies and follow the processes in place to ensure their application of the technologies supports the goals of the organization. (e.g., Database manager, Penetration tester, Asset Management team.)

Using the PRISMA scale, TPPs are assigned a score based on three properties which are, the breadth of coverage, rigor, and strength of protection. The aggregate score of all properties in a TPP represents its maturity value. The maturity of values of related TPPs in a Control is rolled up to get the maturity value of that Control. We refer to the rollup value of the Control as the **maturity score**. The maturity score represents the implementation level of controls in the CSF.

The maturity scores of multiple controls in subcategory and category levels can be further rolled up to generate a new score called "**total maturity**" value, this is used to represent the total level of compliance to a category in the CSF implementation of an organization. The total maturity value represents the strength of security controls an organization might use in mitigating and resisting cyber threats. We assume that the total maturity value generated represents the ability of an organization to resist threats, and it is representative of the resistant strength factor required in the FAIR model. Therefore, we can substitute the estimated resistant strength value with our CSF generated maturity value, as shown in Figure 2.

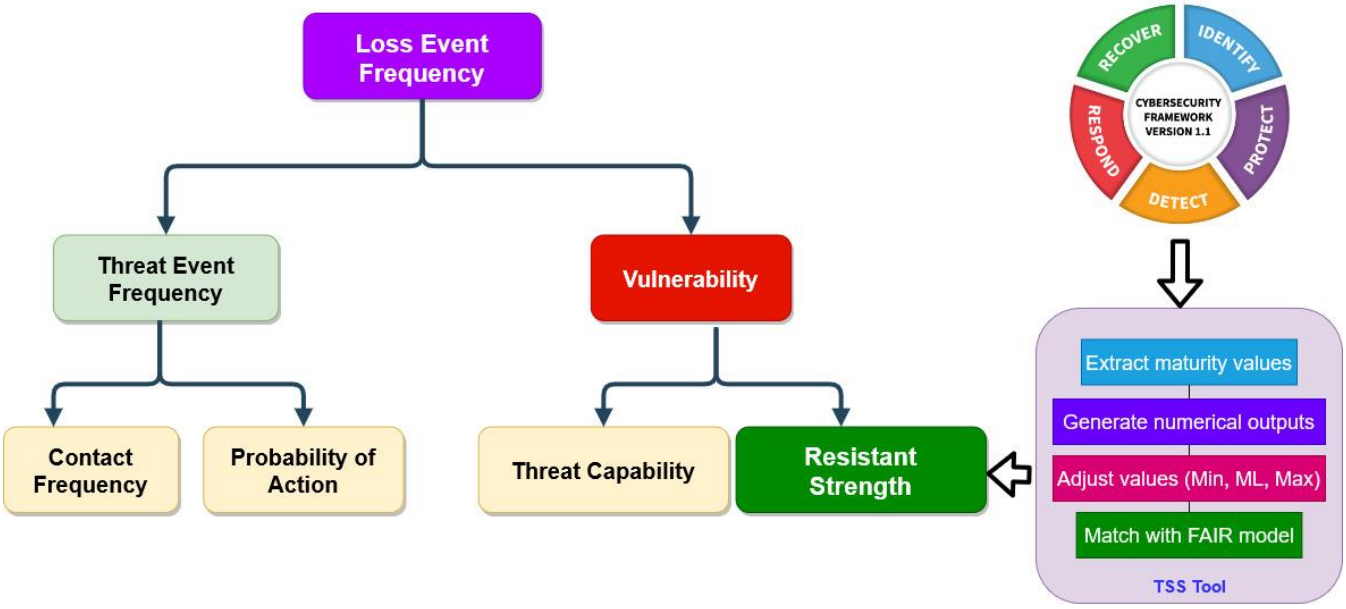

Figure 2: Incorporating NIST CSF into FAIR Model.

4.3 Threat Scenario Simulator Tool

I developed a software tool, Threat Scenario Simulator (TSS), that extends the functionality of the ESM application to integrate the algorithms and structure of the FAIR model into the system, it also accesses the NIST CSF implementation in ESM application to retrieve information about the organizational readiness and security posture. The value of this tool is that it gives a real-time ranking of threat events based on an organization's current security state. The threat ranking generated is specific to the organization's actual security posture and corresponds to the maturity of the organization controls.

In the FAIR framework, security experts provide their opinions as input values for the threat factors components in the risk analysis computation. I confirmed that FAIR's definition of the resistance strength factor is the same as our generated total maturity value, and then substituted FAIR's resistance strength value with the total maturity value extracted from the ESM system. I assume that this is an accurate representation of the organization's control strength in mitigating threats.

As the resistant strength factor in FAIR and total maturity value in CSF are similar, I developed a procedure to extract and incorporate the resistance strength from NIST CSF into the FAIR model. Following this procedure, the total maturity score of a CSF category is used as a substitute for an expert estimated resistant strength value. The method to generate the resistance strength from maturity values of Controls and rolled-up values of their respective subcategories consists of the steps detailed as follow:

Step 1: Identifying threats and mitigation controls:

To ensure the reliability and validation of this method, I applied the method to the same 14 IRENE threat events used by Le et al. (2018), as shown in Table 3. Although the threat events highlighted in Le et al. (2018) were selected for a smart-grid organization, I assumed that the threat events are not specific to only organizations in smart-grid related sectors and as such applies to organizations in other sectors, such as the organization the ESM system was built for. Threat identification is a necessary process if an organization wants to determine the most effective mitigation strategies for probable threats and vulnerabilities it may be exposed to. This is because organizations need to be aware of events that can cause harm or possibly damage their system, and it is also advantageous to know how to respond adequately in a crisis to prevent disastrous consequences. I used the NIST security requirements categories presented in Vasenev et al. (2015) as the mitigation controls that may help mitigate or avoid those threat events. The controls are shown in Table 4.

Table 3: IRENE Threat Events (Le et al., 2018).

ID	Threat Events
1	Perimeter network scanning
2	Information gathering
3	Reconnaissance
4	Craft phishing attacks
5	Spyware/Malware
6	Sniffers/Scanning
7	Insert subverted individuals

8	Exploit physical access
9	Exploit unauthorized access
10	Exploit split tunneling
11	Exploit mobile systems
12	Exploit recent vulnerabilities
13	Physical compromise
14	Hardware compromise

Table 4: NIST Security requirements (Vasenev et al. 2015).

Code	**Mitigation Index**	**Control Name**	**Key phrases**
AC	1	Access Control	User Access Control
AT	2	Awareness and Training	Training based on roles/responsibilities
AU	3	Audit and Accountability	Compliance with policies/requirements
CA	4	Security Assessment and Authorization	Continuous monitoring, Internal checking, Incident investigation.
CM	5	Configuration Management	Change test and management process, Testing of vendor updates
CP	6	Continuity of Operations	Continue/Resume disrupted operations
IA	7	Identification and Authentication	Identification, Authentication
ID	8	Information and Document Management	Protection of digital sensitive data
IR	9	Incident Response	Continue/Resume operations disrupted by an incident
MA	10	Smart Grid Information System Development and maintenance	Maintenance
MP	11	Media Protection	Limit access to media.
PE	12	Physical and Environmental Security	Protect physical assets, Surveillance
PL	13	Planning	Prevent/Recover from interruptions (natural, manmade, equipment)
PM	14	Security Program Management	Implementation of a security program
PS	15	Personnel Security	Staff control, confidentiality agreements
RA	16	Risk Management and Assessment	Identify risks, Identify vulnerabilities
SA	17	Smart Grid information system and services acquisition	Policies for services acquisition
SC	18	Smart Grid Information system and communication protection	Protect communication links
SI	19	Smart Grid information system and information integrity	Manage system flaws, malicious code detection

Step 2: Mapping Threat events to the Mitigation Index

In the process of applying our method, I assumed the smart-grid related controls in Table 4 do not apply to the organization the ESM System was built for, so I eliminated all smart-grid related mitigation controls (Mitigation indexes - 10, 17 , 18 ,19). I proceeded to map the controls presented here to the CSF Subcategories present in the ESM system using the TSS tool, and the mapping is shown in Table 5.

I discovered that the ESM system does not have the exact subcategories specific to the mitigation indexes 3, 5, 6, 7, 11, 12, and 14 to complete a one-to-one mapping. The TSS tool introduced new categories by going down to the Controls sub-level in the ESM-CSF hierarchy and grouping the related controls to form new subcategories. I assumed the ESM and TSS Tool subcategories mappings are representative of the Mitigation index controls.

Table 5: Mitigation Index to ESM Subcategories mapping.

Code	**Mitigation Index**	**Control Name**	**ESM/TSS Tool Subcategories**
AC	1	Access Control	Access Control (PR.AC)
AT	2	Awareness and Training	Awareness and Training (PR.AT)
AU	3	Audit and Accountability	Auditing
CA	4	Security Assessment and Authorization	Risk Assessment (ID.RA)
CM	5	Configuration Management	Configuration Management
CP	6	Continuity of Operations	Continuity of Operations
IA	7	Identification and Authentication	Identification and Authentication
ID	8	Information and Document Management	Data Management (IT.DM)
IR	9	Incident Response	Response Planning (RS.RP)
MP	11	Media Protection	Media Protection
PE	12	Physical and Environmental Security	Physical Security
PL	13	Planning	Recovery Planning (RC.RP)
PM	14	Security Program Management	Security Program
PS	15	Personnel Security	Personnel (IT.PR)
RA	16	Risk Management and Assessment	Risk Management Strategy (ID.RM)

Vasenev et al. (2015) established a one-to-one mapping between a single IRENE threat event and the mitigation indexes that are involved in the process of avoiding, mitigating, and facing the risk posed by those threats. Table 6 shows the IRENE threat events mapping to the mitigation indexes and, by extension, the ESM subcategories.

Table 6: Threat events to Mitigation controls mapping (Vasenev et al. 2015)

ID	Threat Name	Mitigation Index (Table 5)
1	Perimeter network scanning	11, 12
2	Information gathering	11, 2, 8
3	Reconnaissance	2, 4, 7, 12, 16
4	Craft phishing attacks	2, 14, 15
5	Spyware/Malware	5
6	Sniffers/Scanning	4
7	Insert subverted individuals	1, 2, 4
8	Exploit physical access	1, 4, 12, 15
9	Exploit unauthorized access	1, 2, 7
10	Exploit split tunneling	4
11	Exploit mobile systems	16
12	Exploit recent vulnerabilities	8, 10, 13, 16
13	Physical compromise	5, 17, 19
14	Hardware compromise	4, 5, 19

Step 3: Extracting the maturity score

I extracted the maturity scores of the Controls in the ESM subcategories mapped to the mitigation indexes using the TSS tool, and the aggregate score of all Controls in each selected ESM subcategory is used as the maturity score of that subcategory. I developed an algorithm, to provide consistent and precise value, to covert the maturity value derived from the ESM system's NIST CSF implementation to the required quantitative input for the resistant strength factor in the FAIR model, the algorithm is illustrated in Figure 3. I assumed that value generated from the conversion scale represents the expected

value for the resistant strength factor, the Most Likely (ML) value. The ML value was modified to generate the Minimum and Maximum values, respectively, to match the input requirements for the FAIR model.

NOTE: Maturity score is a floating-point digit ranging from 0.0 – 5.0

Conversion scale for Total maturity score to resistant strength
0.0 - 1.0 => 0 -20
1.0 – 3.0 => 20-80
3.0 – 4.0 => 80-90
4.0 - 5.0 => 90-98
The resistant strength value from the scale above is assigned to the Most Likely value in FAIR.

Conversion of ML to Min and Max
Min value = 90% of ML
Max value = 110% of ML

Figure 3: Maturity Score to Resistant Strength Algorithm

Step 4: Generating Resistance Strength value

Using the total maturity scores and the algorithm in Figure 3, I used the TSS Tool to generate the Minimum, Most Likely, and Maximum resistant strength values for the sub-categories identified in the mitigation indexes presented in Table 5. The Min, ML, Max resistant strength values represent the actual security posture of the organization. The three values will be used as the resistance strength values in the FAIR model analysis. The resistant strength values generated with the TSS tool are displayed in Table 7.

Table 7: Threats Events mapped to ESM Resistance Strength

ID	Threat Name	Mitigation Index (Table 5)	Min, ML, Max – Resistance Strength
1	Perimeter network scanning	11, 12	81,90,98
2	Information gathering	11, 2, 8	78,87,96
3	Reconnaissance	2, 4, 7, 12, 16	90, 98, 98
4	Craft phishing attacks	2, 14, 15	74,82,91
5	Spyware/Malware	5	74,82,91
6	Sniffers/Scanning	4	75,83,92
7	Insert subverted individuals	1, 2, 4	80,89,98
8	Exploit physical access	1, 4, 12, 15	84, 93, 98

9	Exploit unauthorized access	1, 2, 7	84, 94, 98
10	Exploit split tunneling	4	75, 83, 92
11	Exploit mobile systems	16	71, 79, 87
12	Exploit recent vulnerabilities	8, 10, 13, 16	83, 93, 98
13	Physical compromise	5, 17, 19	75,83, 91
14	Hardware compromise	4, 5, 19	90,98,98

In order to be consistent with the FAIR implementation, I developed a conversion scale for the popular 5 qualitative input values (i.e., Very Low, Low, Moderate, High, Very High) to the 3 quantitative input values required in FAIR (i.e., Minimum, Most Likely, Maximum). Using the assessment scale presented in Table 2 for quantitative to semi-quantitative conversion, I evenly distributed the semi-quantitative values to get the actual quantitative values as displayed in Figure 4.

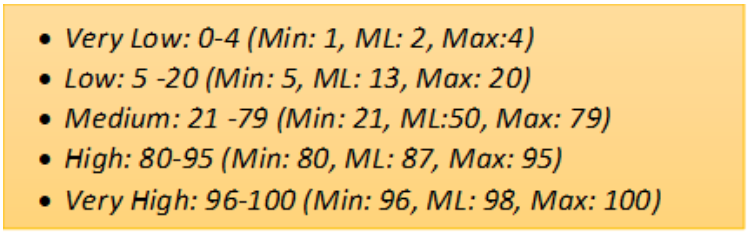

Figure 4: FAIR's Five-point Qualitative to Three-point Quantitative conversion scale.

4.4 Applying the method

The main feature of the TSS tool is its practical implementation of the FAIR model to generate real-time threat ranking results based on an organization's current security state. This tool allows a user to enter values for the FAIR hierarchical elements and performs a simulation of threat events to generate the LEF scores. The details of the theory of operation of this feature are described in The Open Group (2018), it contains the thorough details of the internal operations and algorithms that can be used to produce an acceptable implementation of the FAIR model (a.k.a., Open FAIR™ Risk Analysis (O-RA) standard).

During the application of this method, which consists of steps illustrated in Figure 5, I used the work of Le et al. (2018) as a benchmark because the authors developed the innovative use of the FAIR model's LEF values for threat ranking. Their threat ranking approach was aimed at smart grid networks by incorporating the Bayesian network and FAIR – both quantitative approaches. The method developed in this work is a hybrid approach that involves both quantitative and qualitative analysis frameworks (NIST CSF and FAIR model) to perform a risk assessment. This threat ranking method can be applied to any type of organization with cybersecurity risk management needs.

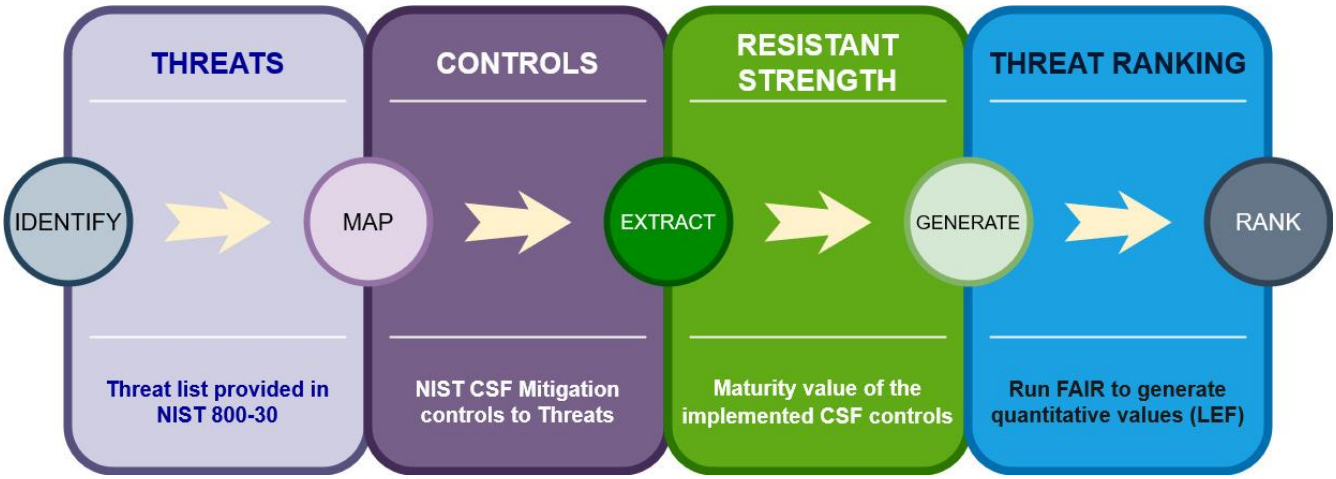

Figure 5: Flow chart of Threats ranking methodology.

For a reliable comparison of results to Le et al. (2018), I maintained the same input values for the first three threat factors, Contact Frequency, Probability of Action, and Threat Capability (CF, PA, TC). I converted them to equivalent quantitative input accepted by our implementation of FAIR using the conversion scale presented in Figure 4. I substituted the last threat factor, resistance strength [RS], with the total maturity score values generated with the TSS Tool using NIST CSF driven data.

The full input values for all four threat factors (CF, PA, TC, RS), displayed in Table 8, is fed into the TSS tool to compute and generate the LEF values for the selected 14 threat events, the LEF values will later be used to rank the threat events. There were two cases where Le et al. (2018) used a range of

values to represent a threat factor value in the quantitative analysis of a threat event. Threat events 9 and 13 had some fuzzy values as inputs, and according to Le et al. (2018), experts could not assign a single state (M or H) for the TC factor in threat 9, so the authors chose 40% M and 60% H. For threat 13, experts couldn't evaluate the PA factor, so the authors chose E, equal probability, for each state (i.e., 20%VL, 20%L, 20%M, 20%H, 20%VH).

Table 8: Converted input states for threat events.

ID	Threat Name	Input States [CF, PA, TC, RS]	TSS Resistance Strength [S] (Table 7)	Converted Input States [CF], [PA], [TC]
1	Perimeter network scanning	[M, H, M, M]	81,90,98	[21,50,79], [80,87,95], [21,50,79],
2	Information gathering	[VH, H, M, H]	78,87,96	[96,98,100], [80,87,95], [21,50,79]
3	Reconnaissance	[M, M, VL, L]	90,98,98	[21,50,79], [21,50,79], [1,2,4]
4	Craft phishing attacks	[H, H, VH, H]	74,82,91	[80,87,95], [80,87,95], [96,98,100]
5	Spyware/ Malware	[M, VH, H, VL]	74,82,91	[21,50,79], [96,98,100], [80,87,95]
6	Sniffers/ Scanning	[M, H, H, M]	75,83,92	[21,50,79], [80,87,95], [80,87,95]
7	Insert subverted individuals	[M, H, H, VL]	80,89,98	[21,50,79], [80,87,95], [80,87,95]
8	Exploit physical access	[L, M, L, H]	84, 93, 98	[5,13,20], [21,50,79], [5,13,20]
9	Exploit unauthorized access	[H, M, 0.4M-0.6H, VH]	84, 94, 98	[80,87,95], [21,50,79], [56,73,89]
10	Exploit split tunneling	[L, H, H, M]	75, 83, 92	[5,13,20], [80,87,95], [80,87,95],
11	Exploit mobile systems	[VH, H, VH, H]	71, 79, 87	[96,98,100], [80,87,95], [96,98,100]
12	Exploit recent vulnerabilities	[H, M, H, VH]	83, 93, 98	[80,87,95], [21,50,79], [80,87,95]
13	Physical compromise	[VL, E, L, VL]	75,83, 91	[1,2,4], [40.4, 50, 59.6], [5,13,20]
14	Hardware compromise	[M, L, H, M]	90,98,98	[21,50,79], [5,13,20], [80,87,95]

For those two cases, I created a unique conversion scale for the range of values given for the TC and PA factors to the Min, ML, and Max input values required by FAIR. I used the conversion scale in Figure 4 as the standard scale to convert the fuzzy values into an acceptable input for FAIR, and assume this calculation is representative of their respective values. The new fuzzy input conversion scale is shown in Figure 6 below.

For 0.4m -0.6H: Value for Min => 0.4 x Medium(Min) + 0.6 x High(Min)
Value for ML => 0.4 x Medium (ML) + 0.6 x High(ML)
Value for Max => 0.4 x Medium (Max) + 0.6 x High(Max)

For E: Value for Min => 0.2 x Very Low(Min) + 0.2 x Low(Min) + 0.2 x Medium(Min) + 0.2 x High(Min) + 0.2 x Very High(Min).
Same applies for ML and Max values.

Calculation
0.4M - 0.6H => (0.4M x 21 + 0.6H x 80), (0.4M x 50 + 0.6H x 88), (0.4M x 79 + 0.6H x 95)
E => Min (0.2VL x 0 + 0.2L x 5 + 0.2M x 21 + 0.2H x 80 + 0.2VH x 96),
ML (0.2VL x 2 + 0.2L x 13 + 0.2M x 50 + 0.2H x 87 + 0.2VH x 98),
Max (0.2VL x 4 + 0.2L x 20 + 0.2M x 79 + 0.2H x 95 + 0.2VH x 100) = 40.4, 50, 59.6

Threat 9 TC input *- 0.4M-0.6H: Min: 56, ML: 73, Max: 89*
Threat 13 PA input *– E: Min: 40.4, ML: 50, Max: 59.6*

Figure 6: Conversion scale for fuzzy input values

SECTION 5: RESULTS

5.1 Results

The cyber threat ranking method outlined in this paper was applied and conducted at one of the business units in a Fortune 500 organization. Table 9 summarizes the features of the organization.

Table 9: Overview of the business unit.[1]

Business Unit Features	
Founded	2007
Average Yearly earnings	$50M
Number of employees	200
Network Infrastructure	VPN, DMZ

The business unit is confirmed to be compliant to NIST CSF 1.1., and I retrieved secure historical data from the organization's database which contained assets, vulnerabilities, threats, and other

[1] To preserve confidentiality and anonymity, we provided minimal details of the business unit.

compliance data- such as NIST CSF's functions, categories, sub-categories, controls, TPPs, TPP scores, their various control states (Fully Implemented, Partially Implemented, Not Implemented, Not Applicable).

Table 10: Numerical results and ranking of Threats events by their LEF values.

ID	Threat Name	Input States [CF, PA, TC, RS]	TSS Tool LEF value	TSS Tool ranking	Ranking from Le et al. (2018)	TSS Tool Resistance Strength
1	Perimeter network scanning	[M, H, M, M]	0	10	7	81,90,98
2	Information gathering	[VH, H, M, H]	0.2	8	4	78,87,96
3	Reconnaissance	[M, M, VL, L]	0	10	10	90,98,98
4	Craft phishing attacks	[H, H, VH, H]	0	10	3	74,82,91
5	Spyware/ Malware	[M, VH, H, VL]	6.5	2	1	74,82,91
6	Sniffers/ Scanning	[M, H, H, M]	5.1	3	6	75,83,92
7	Insert subverted individuals	[M, H, H, VL]	2.59	4	5	80,89,98
8	Exploit physical access	[L, M, L, H]	0	10	13	84,93,98
9	Exploit unauthorized access	[H, M, 0.4M-0.6H, VH]	0.3	7	14	84,94,98
10	Exploit split tunneling	[L, H, H, M]	1.36	6	9	75,83,92
11	Exploit mobile systems	[VH, H, VH, H]	75.54	1	1	71,79,87
12	Exploit recent vulnerabilities	[H, M, H, VH]	1.77	5	8	83,93,98
13	Physical compromise	[VL, E, L, VL]	0	10	12	75,83,91
14	Hardware compromise	[M, L, H, M]	0.04	9	11	90,98,98

I performed a simulation of each threat event scenario individually, by entering the converted input states value into the TSS tool; this produced the respective LEF value for each threat event. The results of all 14 threat scenarios are shown in Table 10. The simulation results show that the top 2 ranked threats, ranked the same as the Bayesian analysis in Le et al. (2018), this gives confidence to the methodology. The method developed in this work correctly identified the first and second threats in the same order as Le et al. (2018) implementation. We can see that threats 1,3,4,8,13 have a LEF value of 0; this is because the resistance strength of our organization is high enough to thwart those threats, and the

tool predicts that none of those threat events will occur based on the current security state of the organization.

5.2 Discussion

We successfully used the hybrid threat ranking method implemented in the TSS tool to identify the most critical threat events to the organization. The threat events 5 and 11 are currently the most severe threats, and we also identified the controls that can defend against the threat events through the threat-to-controls mapping in Table 6. We recommend that the organization's stakeholders should prioritize the improvement of controls in the ESM subcategories "Configuration Management" and "Risk Management" to reduce the exposure to threat events 5 and 11, respectively.

We were able to ascertain that the methodology works by fixing the inputs as same with Le et al. (2018); this helps validate that our method is reasonable. The input values for the four threat factors [CF, PA, TC, RS] used in the computation of the LEF values are expert opinions gotten from Le et al. (2018), I discovered that the input values for the first three threat factors [CF, PA, TC] are applicable and usable in other organizations outside the smart grid sector, but the RS factor is totally dependent on the actual security posture (control strength) of each individual organization. Therefore, using the same values as Le et al. (2018) for the first 3 factors, I substituted the RS value with the total maturity value generated from the TSS tool. An idea for other researchers is to determine the input values of the first three threat factors [CF, PA, TC] based on intelligence gathering or predictive analysis. E.g., An official source could periodically provide values for the threat event frequency, and threat capability factors of most popular threats, or an organization can carry out a periodical survey requiring experts to estimate the values for those factors.

The method in this thesis provides a repeatable and clear path to reach conclusions on the severity of threats to an organization based on their actual resistance strength, and the existence of the hybrid threat ranking approach outlined in this thesis will be helpful to an organization. The cybersecurity

stakeholders can also declare a threat threshold based on the LEF values and ranking of threat events; this will make the decision process easier for executives when deliberating on which threat event mitigation takes the highest priority. The threat threshold approach can also help reduce the list of threats to consider when making decisions.

Organizations will benefit from using this threat ranking method because they will have the ability to identify the most critical threats they might be exposed to, and they can easily focus and prioritize resources on the infrastructure or system to improve security posture against threats with the highest severity. The goal of this thesis is not to challenge the security expert opinions but to encourage organizations to employ NIST CSF controls, and use NIST driven values into quantitative models like the FAIR model to generate Loss Event Frequency values which will give information on threats severity and will be used to rank the threats based on the current security state of the organization.

SECTION 6: CONCLUSION

6.1 Conclusion

This thesis presented a method to rank cyber threats based on the actual security posture of an organization by incorporating NIST CSF driven values into the FAIR model to obtain the LEF values through quantitative assessments. The results derived from ranking cyber threats using the hybrid method in this work confirmed my hypothesis that “Integrating NIST CSF and FAIR to form a hybrid risk assessment approach will create a pragmatic cyberthreat ranking based on the actual security posture of an organization.”

Using the TSS tool developed in this thesis, the researcher can communicate to an organization what threat events they are ready/not ready for and recommend mitigation controls that may help prevent those threat events. The security stakeholders in an organization can now make data-informed

decisions on improving security measures, policies, and programs based on threat's severity with respect to their current actual security posture. One of the main objectives of this work is to convince the security community to embrace the integration of NIST-driven values into quantitative models like the FAIR model.

6.2 Future Work

The hybrid analysis method created in this study is open to adaptation and refinement for further research. Some suggestions for future work are to: focus on extending our method to accommodate more threat events by incorporating known public vulnerabilities and threats such as the CVE dataset of threats and vulnerabilities (CVE, n.d.), expand the complexity of the FAIR probability distribution for a more granular assessment (e.g., Bayesian-FAIR). Other researchers can also develop alternative methods to dynamically generate the inputs for the other three factors [CF, PA, TC]; this will further reduce dependency on expert opinions in computational models.

REFERENCES

Alali, M., Almogren, A., Hassan, M. M., Rassan, I. A. L., & Bhuiyan, M. Z. A. (2018). *Improving risk assessment model of cyber security using fuzzy logic inference system*. Computers & Security, 74, 323-339. doi:10.1016/j.cose.2017.09.011

Aven, T. (2015). *Risk assessment and risk management: Review of recent advances on their foundation.* Eur J Oper Res 253:1–13

Bowen, P., Kissel, R. (2007). *NISTIR 7358 - Program Review for Information Security Management Assistance (PRISMA)*. https://doi.org/10.6028/NIST.IR.7358

Barrett, M.P. (2018). *NIST Cybersecurity Framework: Framework for Improving Critical Infrastructure Cybersecurity - version 1.1*. https://doi.org/10.6028/NIST.CSWP.04162018

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., Stoddart, K. (2016). *A review of cyber security risk assessment methods for SCADA systems*. Comput. Security, 56, pp. 1-27. https://doi.org/10.1016/j.cose.2015.09.009.

Clark, K., Tyree, S., Dawkins, J., Hale, J. (2004). *Qualitative and quantitative analytical techniques for network security assessment*. In: information assurance workshop IEEE, 2004. pp 321–328

CVE (Common Vulnerabilities and Exposures). (n.d.). Retrieved November 11, 2019, from https://cve.mitre.org/

Dimensional Research. (2016). *Trends in security framework adoption: A survey of IT and Security professionals*. Retrieved October 15, 2019, from https://static.tenable.com/marketing/tenable-csf-report.pdf

Executive Order 13636. (2013). *Improving Critical Infrastructure Cybersecurity*. Retrieved from http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf

FAIR-U Analysis. (n.d.). Retrieved September 12, 2019, from https://app.fairu.net/

FAIR Institute Blog. (2019). *NIST Maps FAIR to the CSF: Big Step Forward in Acceptance of Cyber Risk Quantification*. Retrieved December 12, 2019, from https://www.fairinstitute.org/blog/nist-maps-fair-to-the-csf-big-step-forward-in-acceptance-of-cyber-risk-quantification

Farahmand, F., Navathe, S.B., Sharp, G.P., Enslow, P.H. (2005). *A management perspective on risk of security threats to information systems*. Inf Technol Manag 6:203–225

Fenz, S., Heurix, J., Neubauer, T., Pechstein, F. (2014). *Current challenges in information security risk management*. Information Management & Computer Security, Vol. 22 Issue: 5, pp.410-430. Retrieved from https://doi.org/10.1108/IMCS-07-2013-0053

Figueira, P.T., Bravo, C.L., López, J.L.R. (2020). *Improving information security risk analysis by including threat-occurrence predictive models*. Computers & Security, Vol 88, 101609, ISSN 0167-4048. https://doi.org/10.1016/j.cose.2019.101609

Freund, J., Jones, J. (2015). *Measuring and Managing Information Risk: A FAIR Approach (1st ed.)*. Oxford, U.K.: Butterworth-Heinemann.

Gabriel, A., Shi, J., & Ozansoy, C. (2017). *A proposed alignment of the national institute of standards and technology framework with the funnel risk graph method*. IEEE Access, 5, 12103-12113. doi:10.1109/ACCESS.2017.2718568

Hiller, J.S., & Russell, R.S. (2017). *Privacy in crises: The NIST privacy framework*. Journal of Contingencies and Crisis Management, 25(1), 31-38. doi:10.1111/1468-5973.12143

IASCA. (2012). *COBIT 5*. Retrieved October 20, 2019, from https://cobitonline.isaca.org

Ibrahim, A., Valli, C., McAteer, I., & Chaudhry, J. (2018). *A security review of local government using NIST CSF: A case study*. The Journal of Supercomputing, 74(10), 5171-5186. doi:10.1007/s11227-018-2479-2.

ISA. (2009). ANSI/ISA-99.02.01-2009. Retrieved October 20, 2019, http://www.icsdefender.ir/files/scadadefender-ir/paygahdanesh/standards/ISA-62443-2-1-Public.pdf

ISA. (2012). ANSI/ISA-62443-3-3 (99.03.03)-2013. Retrieved October 20, 2019, http://www.icsdefender.ir/files/scadadefender-ir/paygahdanesh/standards/ISA-62443-3-3-Public.pdf

ISO. (2013). *ISO/IEC 27001:2013*. Retrieved October 20, 2019, from https://www.iso.org/standard/54534.html

Jones, J. (2016). *A review of NIST CSF*. Retrieved from https://www.fairinstitute.org/blog/nist-csf-fair-part-2

Kaspersky Lab. (2015). *Global IT Security Risks Survey*. Retrieved October 15, 2019, from https://media.kaspersky.com/pdf/global-it-security-risks-survey-2015.pdf

Krishan, R. (2018). *Corporate solutions to minimize expenses from cyber security attacks in the united states*. Journal of Internet Law, 21(11), 16-19.

Le, A., Chen, Y., Chai, K.K., Vasenev, A., Montoya, L. (2018). *Incorporating FAIR into Bayesian Network for Numerical Assessment of Loss Event Frequencies of Smart Grid Cyber Threats.* Mobile Netw Appl. https://doi.org/10.1007/s11036-018-1047-6

Marsh Microsoft Global Cyber Risk Perception Survey. (2019). Retrieved Jan 17, 2020, from https://www.microsoft.com/security/blog/wp-content/uploads/2019/09/Marsh-Microsoft-2019-Global-Cyber-Risk-Perception-Survey.pdf

National Institute of Standards and Technology. (2012). NIST Special Publication 800-30 Rev 1: Guide for Conducting Risk Assessments. Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

National Institute of Standards and Technology. (2014). *Assessing security and privacy controls in federal information systems and organizations - SP 800-53*. Retrieved October 20, 2019, from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf

National Institute of Standards and Technology. (2014). *Framework for improving critical infrastructure cybersecurity: Version 1.0*. Retrieved October 20, 2019, from http://www.nist.gov/sites /default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

National Institute of Standards and Technology. (2019). *Cybersecurity Framework: Informative Reference Catalog*. Retrieved from https://csrc.nist.gov/Projects/Cybersecurity-Framework/Informative-Reference-Catalog

NIST CSF Online Learning. (n.d.). *Uses and Benefits of the Framework*. Retrieved November 15, 2019, from https://www.nist.gov/cyberframework/online-learning/uses-and-benefits-framework

Ponemon Institute. (2018). *Cost of Data Breach Study: Impact of Business Continuity Management*. Retrieved from https://www.ibm.com/downloads/cas/AEJYBPWA

Shameli-Sendi, A., Aghababaei-Barzegar, R., Cheriet, M. (2016). *Taxonomy of information security risk assessment (ISRA)*. Comput Secur 57:14–30

The Open Group. (2009). *Technical Standard: Risk Taxonomy*. Retrieved from https://pubs.opengroup.org/onlinepubs/9699919899/toc.pdf.

The Open Group. (2018). *Open FAIR™ Tool with SIPmath™ Distributions: Guide to the Theory of Operation*. Retrieved from https://publications.opengroup.org/g181

Vasenev, A. et al. (2015). *D2.1: Threats identification and ranking, Improving the Robustness of Urban Electricity Networks IRENE*. Retrieved from http://ireneproject.eu/wp-content/uploads/2016/01/IRENE-D2.1.pdf

Wang, J., Neil, M., Fenton, N. (2019). *A Bayesian Network Approach for Cybersecurity Risk Assessment Implementing and Extending the FAIR Model*. Computers & Security. https://doi.org/10.1016/j.cose.2019.101659

Wheeler, E. (2011). *Security Risk Management: Building an Information Security Risk Management Program from the Ground Up* (Kindle Location 828). Elsevier Science. Kindle Edition.