Integrating NIST Framework into FAIR model for Quantitative Risk Assessment of Cyber Threats

Adeyinka Bakare
School of Information Technology
University of Cincinnati, OH. USA
bakareal@ucmail.uc.edu

Vivek Kunapareddy
Department of Computer Science
University of Cincinnati, OH. USA
kunapavk@ucmail.uc.edu

Yahya Gilany
School of Information Technology
University of Cincinnati, OH. USA
gilanyym@ucmail.uc.edu

Hazem Said
School of Information Technology
University of Cincinnati, OH. USA
saidhm@ucmail.uc.edu

ABSTRACT

As incessant cyber-attacks on organizations increase in complexity and destructiveness with the aim to disrupt services and steal information, proactive measures are critically needed to mitigate these attacks, cyber security risk assessment tops the list of measures. This study provides an overview of cybersecurity risk assessment, various types of frameworks, and the difference between qualitative and quantitative cybersecurity risk assessments. The aim of this early research is the creation of a hybrid system which integrates an existing cybersecurity risk assessment system based on the NIST framework into the Factor Analysis of Information Risk (FAIR) model, an analytic risk assessment model that enables true quantitative measurement. In this study, we propose a hybrid-

IT Research Symposium'19 Extended Abstracts, April 9, 2019, Cincinnati, Ohio, USA.

KEYWORDS

Cyber threat; Resistance strength; Annual Loss Expectancy; Quantitative Risk Assessment.

assessment tool which will be used to describe and compare the impact of using NIST driven values as inputs for the resistance strength to determine the Loss Event Frequent (LEF) and Annual Loss Expectancy (ALE) of a risk scenario as opposed to using experts' opinion as user inputs for determination of the LEF and ALE values.

INTRODUCTION

All corporations are concerned with the growing risks associated with cyber-attacks. Studies shows that a single data breach will cost an average organization over $3million and most attacks targets confidential and financial information, or intellectual properties of companies. With so much enormous consequences, it is conspicuous to say that, cybersecurity risk assessment plays a crucial role in the information security system of any organization. These circumstances prompted the POTUS to sign an Executive Order [4], which deals with improving cybersecurity risk management and IT modernization in the country. When a comprehensive cyber risk assessment is performed, the organization understands their current level of cybersecurity risk, then they can take sophisticated and prioritized steps to improve it. In the USA, NIST is the cybersecurity risk assessment framework used by most public and private organizations to ensure compliance with industry standards. But the major limitation with this framework is the lack of an analytic capability that would allow its users to quantify cybersecurity risks as well as compliance gaps in their organizations. The purpose of this study is to introduce and integrate FAIR model together with the current cybersecurity risk assessment system of an organization. FAIR is an analytic model that enables true quantitative measurement of an organization's cyber risk assessment [6], this allows them to evaluate and measure the significance of gaps in compliance to industry standards, so that they can make well-informed choices about how and where to utilize their limited resources.

REVIEW OF RELATED LITERATURE

This literature review includes three areas of focus: (a) empirical studies of cybersecurity threats and risks (b) cyber risk frameworks, and (c) comparison between the qualitative and quantitative approaches of cybersecurity risk assessments. This review is limited to risk assessments systems that have a standard cybersecurity risk framework. Studies targeting the development of a new framework are excluded.

Cybersecurity Threats and Risks

There is a huge rise in sophistication of cyber-attacks recently and corporate organizations in the United States are greatly affected by this [10]. Research shows that it takes an average of 46 days to resolve a cyber-attack or security breach, which translates to $21,155 loss per day. These costs present a huge liability to organizations and it can escalate into more disastrous consequences. This

brings about the urgent need to develop a specialized cyber security risk assessment model that will help to identify, mitigate and possibly prevent losses to the incessant cyber threats [1].
Many researchers have studied several risk frameworks as well as their advantages. Some researchers proposed that an integrated framework will be of economic advantage to an organization [7], another recommended the creation of specialized risk analysis system and incident support teams, to tackle cyber threats [10].

Cybersecurity Risk Frameworks

Measuring how efficient and effective security frameworks are toward managing real life cybersecurity risk is crucial to understanding its economic impact to any organization [14]. It is necessary for organizations to take a systematic approach in implementing a risk management framework [8]. The studies reviewed investigated the top cyber risk frameworks available as well as their effectiveness. A study [9] analyzed five related cybersecurity frameworks (NIST SP 800-53 Rev. 4., Control Objectives for Information and Related Technologies (COBIT5), ISO/IEC 27001:2013, ISA 62443-2-1:2009, SA 62443-3-3:2013) with case study examples of their implementation. It was noticed that NIST CSF offers more advantages by leveraging and integrating other frameworks.
NIST CSF is the preferred framework used by most organizations because it is designed to evolve with changes in cybersecurity threats, processes, and technologies. These organizations usually design assessment tools based on the NIST CSF model, which they can use to target areas of an organization to measure its risk level. The tool's major function is to determine the level of compliance of an area of an organization, and it was used to evaluate the organization's system studied in [9] and successfully identified the risks/possible threat areas.

Integrating NIST on other models

In [1], the researchers implemented their own algorithm/models on NIST framework to make it more efficient. Threat modelling was used to identify, quantify and analyze the possible risks of a computer-based system, by identifying the most important assets in the system, the threats to each component and respectively rank them by their risk probabilities- but this was still a qualitative approach. Another researcher attempted to align the NIST framework with the FRGM in one approach which was proposed to minimize or eliminate loss to an organization [9].
A method was presented in [11] to incorporate the FAIR 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 manager can then formulate a more effective mitigation plan, which includes the most cost-effective security countermeasures to lower the threats' impacts. As observed by [11], most organizations typically apply the qualitative approach, others apply the quantitative approaches available.

Qualitative Approach to Assessment of Cybersecurity Risks

In practice, most cybersecurity risk frameworks perform a qualitative risk assessment; this is mainly a process of using ordinal rating scales (e.g., 1-5; green, yellow, red; low, medium, high; etc.) to plot various risks based on their frequency (likelihood of occurrence) and magnitude (impact of loss) to the organization. Going by this, organizations can visually represent the relative severity of the various risks the organization faces. Although, qualitative risk assessment is efficient, useful in making quick decisions, and easy to communicate (with a pretty heat map), the drawbacks associated with it are bias and inconsistencies in risk analysis, 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 do you decide which to mitigate first? Which one is "reddest"? Succinctly, the qualitative approach presents a systematic analysis to give a qualitative output rather than a numerical result [3]. Their main advantage is the reliable reasoning; however, in many cases, the output is not detailed enough to take clear decisions [12].

Quantitative Approach to Assessment of Cybersecurity Risks

On the other hand, 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 (dollars and cents) as its measurement, rather than an ordinal or relative scale. Quantitative measures enhance the analysis by scoring the effectiveness of current and potential security solutions as confirmed in [3]. The objective of the quantitative assessment is to utilize probability theory and statistics to assign numerical probabilistic values to threat likelihood [5]. Although this method provides clear guidance about the threat, it usually has high difficulty in implementation and ambiguity evaluation [13].

The leading quantitative cyber risk analytics model is the FAIR model, it's definitions of risk is related to the same in [2]. By using a structured model, as shown in Fig. 1, to evaluate risk, FAIR helps to ensure that the same rigorous and consistent approach is used across analysis, as such, allowing them to be accurately compared. [6] best described this model as, "You can't effectively and consistently manage what you can't measure, and you can't measure what you haven't defined".

PROBLEM STATEMENT/RESEARCH QUESTION

Based on the review of related literature, it is evident that there is an urge for a combination both approaches to create a hybrid cybersecurity risk assessment approach. Studies shows that very few works have ventured into the development of an assessment tool that is based on a hybrid approach. This study proposes such a tool and aims to answer the following research question:

What is the impact of using NIST driven values as input for the resistance strength to determine the annual loss expectancy?

Figure 1: Structure of FAIR MODEL

RESEARCH METHOD

The novelty of this early study is the creation of a hybrid cybersecurity risk assessment tool that combines the qualitative and quantitative approaches of cybersecurity risk assessment identified in the review of previous literature. This research proposes to use a case study of an organizational business unit to create a risk scenario, then identify the business assets and costs, threats and threat actors of the hypothetical risk, also identify the controls in place to mitigate such threats in the organization. The tool will perform an assessment of the business unit based on the NIST framework, the results will be used as input data to perform a quantitative assessment based on the implementation of FAIR model, which uses the Monte-Carlo simulation engine as well as the Binomial and Metalog probabilistic distributions.

This study will use a structured survey of cybersecurity experts and entry-level analysts to get their estimation of the minimum, most likely and maximum maturity values of the controls in the business unit, which will be used as input data for the FAIR model implementation to derive the Vulnerability, Loss Event Frequency (LEF), Loss Magnitude (LM) and Annual Loss Expectancy (ALE).

CONCLUSION

In this early study, we looked at the related literature in the realm of cybersecurity risk assessment. We proposed a hybrid cybersecurity assessment tool that combines both quantitative and qualitative approaches, and our future expectation is that the results derived from using NIST driven data should be very close to the results gotten from experts' opinion, also it should be far off from the results gotten from the entry-level analysts. The impact of this study will be to enable all cybersecurity analysts, not just experts, make efficient use of the FAIR model by utilizing NIST driven

ACKNOWLEDGEMENTS

The authors would like to express their gratitude to the Information Technology Solutions Center for providing the environment and support to conduct this study.

data, which will allow everyone in the organization to get an accurate ALE, which represents the financial loss they are exposed to in a risk scenario. This also makes the experts' opinion on the quantitative assessment using FAIR model more accurate and not undervalued.

REFERENCES

[1] 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

[2] Aven T (2016). Risk assessment and risk management: Review of recent advances on their foundation. Eur J Oper Res 253:1–13

[3] 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

[4] Executive Order 13636: Improving Critical Infrastructure Cybersecurity, 2013, [online] Available: http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf

[5] Farahmand F, Navathe SB, Sharp GP, Enslow PH (2005). A management perspective on risk of security threats to information systems. Inf Technol Manag 6:203–225

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

[7] 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

[8] 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

[9] 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

[10] Krishan, R. (2018). Corporate solutions to minimize expenses from cyber security attacks in the united states. Journal of Internet Law, 21(11), 16-19. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=iih&AN=131103585&site=ehost-live

[11] Le, A., Chen, Y., Chai, K.K. et al. (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

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

[13] Stefan Fenz, Johannes Heurix, Thomas Neubauer, Fabian Pechstein, (2014) "Current challenges in information security risk management", Information Management & Computer Security, Vol. 22 Issue: 5, pp.410-430, https://doi.org/10.1108/IMCS-07-2013-0053

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