Module 12: Activity 9

“Harsh Manishbhai Siddhapura”

“Vaibhavi Nitin Honagekar”

“Arunava Lahiri”

“Thembelihle Shongwe”

“Sai Shashank Nagavaram”

“Anandha Krishnan Senthooraan”

“Group: Class96958 4”

“Ira A. Fulton School of Engineering, Arizona State University”

“IFT 520: Advanced Information Systems Security”

“Prof. Upakar Bhatta”

November 15, 2023

Mitigating Cyber Attacks:

Creating, Developing, and Empirically Testing

Cybersecurity Skills Index for Non-IT Professionals

Introduction

Organizations are facing an increasing number of cyber threats, most of which are caused by staff members who are not knowledgeable about cybersecurity. The study highlights the vital requirement of evaluating and enhancing non-IT staff members' cybersecurity competencies in order to stop vulnerabilities and breaches that might cause financial and operational losses. It offers the Cybersecurity Skills Index (CSI) as a way to evaluate people's cybersecurity, especially non-IT workers. The study acknowledges the involvement of employees in both intentional and illicit actions and highlights the importance of enhancing cybersecurity capabilities.

This article highlights the fundamental issue with cybersecurity and how it directly affects human error, showing how people are typically the weakest link in a company's security system. He underlined the impact of human error, social engineering, and inappropriate conduct on cybersecurity, asserting that up to 95% of cyberthreats to businesses are caused by people with inadequate cybersecurity knowledge. The purpose of these research was to develop and improve the Cybersecurity Skills Index (CSI), a tool that evaluates non-IT personnel' cybersecurity proficiency. The purpose of the application was to address the cybersecurity risk posed by inexperienced workers.

The Cybersecurity capabilities Index (CSI), a tool for evaluating the cybersecurity capabilities of non-IT personnel, is explained in the article that follows. This study focuses on those who contribute significantly to protecting organizations from cybersecurity threats but are not directly involved in IT. This paper explains the development and application of the instrument and offers a means of assessing people's cybersecurity proficiency. This article's goal is to provide a comprehensive analysis of the development and validation of the Cybersecurity abilities Index (CSI) tool, which is designed to evaluate non-IT workers' cybersecurity aptitude. There has never been a more pressing need for cybersecurity measures in our increasingly digital society, full of online threats and weaknesses.

The main objective of this research is to develop a CSI tool that presents a negative impression of the cybersecurity proficiency of non-IT personnel. The tool uses a scenario-based evaluation to find out how competitive you are in the cybersecurity area. It consists of written scenarios and hands-on activities. Most importantly, as these exercises become more complex, the application can determine who is the most proficient student in a particular cybersecurity course. An important component of this study, which describes the exacting method employed to achieve this objective, is the tool's validation. Through the Delphi process, experts (SMEs) come to a consensus to confirm that the tool's events and actions are legitimate and pertinent to issues facing the actual world.

The impact of participants' demographics on their cybersecurity abilities is also covered in this article. It examines elements including age, gender, education, usage of technology, and characteristics specific to a profession. These occasions are essential for the advancement of cybersecurity skills among non-IT workers. Intelligence is divided into Business Information (WIS), Malware, and Personally Identifiable Information (PII) using detailed average ratings. The average score for the Cybersecurity Skills Index (CSI) is 59.8, which represents the overall performance of all the indicators put together.

Concepts

The combination of knowledge, skills, and abilities that allow someone to securely handle electronic information and communicate well is referred to in this article as cybersecurity competencies. It highlights how important monitoring protocols are to demonstrating cybersecurity skills. The aim of this study was to develop a framework of job-based criteria for evaluating non-IT workers' cybersecurity skills so that businesses may better protect themselves from dishonest employees.

This essay explores a number of topics about cybersecurity skills and their importance. Self-report indicators should be used to test traditional IT abilities, but the focus should be on the need for more impartial and objective evaluation methods, like the CSI. Technical knowledge of hardware, software, and information technology operations is referred to as IT skills. The article states that responsibility and aptitude are both essential for success and have a significant impact on employee performance and productivity. Cybersecurity skills are critical since organizations depend on IT for daily operations. This essay also discusses the value of real-world experience in providing objective evidence of aptitude.

In addition, the article provides data and numbers to support its findings. 173 non-IT professionals participated in the evaluation at the beginning, which employed CSI verification techniques. There was a significant gender gap: 103 women and 70 men participated. Most of the participants utilize the Internet, and most are in the age range of 20 to 64. In addition to performance differences across nine measures, this article offers average ratings for critical cybersecurity competencies.The ability to prevent private information from leaking out received the highest grade, while the ability to stop PII from being stolen through unsecured websites received the lowest. With average scores for each, intelligence is divided into three categories: business information, malware, and personally identifiable information.

The need of comprehending and enhancing the cybersecurity skills of non-IT workers is emphasized by this study. Using the CSI prototype tool, organizations and decision makers may get guidance on how to prepare cybersecurity workers, especially those who are susceptible to social engineering and cyber attacks. The essay recommends emphasizing education and training to improve these people's cybersecurity skills and, therefore, the organization's defenses against cyberthreats. It highlights the vital position that non-IT specialists play in cybersecurity administration and the significance of continuous evaluation and advancement in this area.

- **Cybersecurity Skills Assessment:** Creating a tool (CSI) to evaluate non-IT personnel' cybersecurity proficiency is the main objective. This involves assessing the person's ability to do certain cybersecurity tasks.
- **Scenario-Based Assessment:** Research suggests that activities and situations may be utilized to assess cybersecurity proficiency. This approach provides more accurate findings than standard survey-based evaluations.
- **Incremental Difficulty:** This study adopts the stance that tasks including all cybersecurity competencies are growing increasingly complex. Subsequently, the system may indicate which people are the most advanced by highlighting tasks that exceed their skills.
- **Validation:** The research, which employs the Delphi method, focuses on how experts (SMEs) use tools. An experiment was conducted to verify the validity of the scale.
- **Demographic Factors:** This study examined the relationship between cybersecurity engagement and demographic parameters such as age, gender, education, and technology use.

Facts and Statistics

The pamphlet is filled with astounding statistics and information that highlight the severity of the issue. Reports state that between 72 and 95 percent of cyber threats to companies are the result of human error brought on by a lack of cybersecurity expertise. It is widely believed that people represent a crucial security vulnerability in an organization, and social engineering tactics are often used to get beyond sophisticated intrusion detection systems. The letter also warns that workers may still be open to assaults even with the best security procedures in place because of a lack of security equipment, inexperience, or human error. It highlights the growing importance of cybersecurity training programmes and the need to improve the skills of cybersecurity experts via instruction and training.

The study's innovation is in establishing the validity and usefulness of the Cyber Security abilities Index (CSI) as a tool for evaluating professionals' cyber security skills. Not IT. These solutions help businesses mitigate assaults, stop vulnerabilities, and stop breaches brought on by a lack of cybersecurity experts. As part of this study, the Cybersecurity Skills Index (CSI) instrument was developed and validated. Its purpose is to quantify the cybersecurity skills of non-IT personnel. The tool integrates actions based on recorded occurrences in order to stay competitive in the cybersecurity business. Eight SMEs were asked to evaluate the activities, and they gave insightful and helpful comments. Every cybersecurity skill is discussed independently, with increasing degrees of difficulty in the exercises.

The goal of the CSI tool is to ascertain each participant's highest level of competence in each cybersecurity domain. The tool was rigorously tested during its development, and the Delphi technique was used to get agreement among SMEs. To ensure the accuracy of the ratings provided by the sample tool, a pilot study was conducted. In the third phase, which concentrated on the southern United States, 975 workers from various organizations were surveyed using the CSI instrument. Age, gender, use of the internet, and principal employment were all regarded as demographic factors. The results showed that "Preventing confidential digital information from being disclosed to unauthorized persons" was the skill with the highest mean score, while "Protecting Personal Information from visiting unsecured websites" had the lowest mean score.

The data breach alert report states that insider threats, bad conduct, or human error are the main causes of breaches. He continued by saying that people are better at identifying and reporting instances of cyberespionage than internal processes or technology. The claims that millions of personal details have been compromised in documented occurrences are what have sparked the conversation about data breaches. Additionally, data indicates that evaluating staff members' cybersecurity skills is essential for mitigating and recovering from cybersecurity incidents and, ultimately, ensuring business continuity. It looks at the relationship between risk mitigation and cybersecurity intelligence inside the NIST cybersecurity framework.

The article provides various facts and statistics, including:

- Eight small and medium-sized firms (SMEs) contributed to the development and implementation of the CSI model tool by providing constructive and pertinent input on the events, activities, and scores.
- The tool uses four exercises with varying degrees of difficulty to evaluate nine cybersecurity talents, each provided individually.
- Of the lay professionals in IT, 173 utilize standard design tools.
- There were 70 men (40.5%) and 103 women (59.5%) among the participants.
- Participants ranged in age from 20 to 64, with 83.2% of them fitting this description.
- The highest score (81.0%) went to protection against the leakage of private information, while the lowest score (45.1%) went to protection against unauthorized access to personal information.
- Information processing (WIS), malware, and personally identifiable information (PII) are the three areas into which intelligence is divided. These categories have average scores of 72.5%, 51.3%, and 56.1%, respectively.
- A score of 59.8 on the General Cyber Security Skills Index (CSI) represents the average.

Summary and Conclusions

This article's conclusion acknowledges the crucial role that staff members play in cybersecurity organizations and aims to uncover skills through the development and testing of CSI. This study is important because it will provide organizations with practical techniques to evaluate and enhance the cybersecurity skills of non-IT staff, hence reducing cyberthreats and criminal risks. An overview of important subjects pertaining to cybersecurity capabilities, measurement, and their impact on corporate security is provided in this article. presents the novel concept of CSI as a tool for assessing the network security expertise of non-IT personnel, with the aim of reducing the risk of network hazards brought on by information leakage and skill gaps.

An overview of the development and validation of CSI instruments for evaluating cybersecurity proficiency in non-IT personnel is provided in this chapter. Adding challenging activities and scenario-based analysis increases the assessment's accuracy even further. The importance of identifying and enhancing the cybersecurity skills of those who are susceptible to social engineering and cyberthreats is emphasized by this study. This study explores the need for education and training to reduce cyber risk as well as the demographic traits that affect cybersecurity ability. By reviewing the results, organizations may identify any areas where staff members may need further training to improve their readiness for cybersecurity. The CSI prototype tool is helpful in assessing and improving the cybersecurity knowledge of non-IT professionals.

Overall, this study highlights the need of assessing and educating non-IT staff members in cybersecurity to strengthen the organization's defenses against cyberattacks and stresses the critical role that employees play in cybersecurity management. This article describes how the Cybersecurity Skills Index (CSI), a tool for evaluating the cybersecurity skills of non-IT personnel, was developed and validated. The tool has been reviewed by a group of eight specialists (SMEs) and is based on operational situations that provide cybersecurity risks. Because all cybersecurity skills are provided in a step-by-step manner, the tools are able to evaluate each participant at their highest potential. In addition to thorough testing and validation, a research study was conducted to improve the ratings' accuracy throughout the creation of the CSI tool. In the third stage, 975 employees from various organizations in the eastern United States were surveyed on a variety of topics, including employment, Internet use, primary occupation, and age and gender.

The results vary according to the level of expertise, with "Protecting Personal Information from visiting unsecured websites" receiving the lowest score and "Policy to prevent confidential digital information from being disclosed to unauthorized persons" receiving the best score. These results suggest that non-IT workers are ready for public events that might affect their cybersecurity knowledge and skills. By enhancing the cybersecurity skills of non-IT staff, businesses may reduce the likelihood of data breaches brought on by social engineering or human mistake with the use of CSI technology. These tools, which provide a way to find and address competency gaps, may introduce unforeseen cybersecurity threats in an increasingly digital world.

References

Lerouge, C., Newton, S. and Blanton, J.E. (2005), “Exploring the systems analyst skill set: perceptions, preferences, age, and gender”, *The Journal of Computer Information Systems*.

Kvedar, D., Nettis, M. and Fulton, S.P. (2010), “The use of formal social engineering techniques to identify weaknesses during a computer vulnerability competition”, *Journal of Computing Sciences in Colleges*.

Jang-Jaccard, J. and Nepal, S. (2014), “A survey of emerging threats in cybersecurity”, *Journal of Computer and System Sciences.*