IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 9, September 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.524

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 9, September 2024

|DOI: 10.15680/IJIRSET.2024.1309068|

A Quantitative Research Method on the Future Cybersecurity Workforce, Going Beyond Technical Skills for Successful Cyber Performance

Nabanita Das

Senior Software Engineer & PhD Student, National University, Chicago, United States

ABSTRACT: An evaluation of research must be conducted from a fundamental point of view to ensure its efficiency. Finding solutions to the real problems will be facilitated by understanding them, analyzing them, and analyzing the solutions. A qualitative study analyses words rather than numbers to understand some aspect of social life as part of its goal. A qualitative approach might seem unclear to those more familiar with quantitative approaches since quantitative methods strive to measure something. Depending on many factors such as location, test data, security concerns, etc., how we conduct our research is key to analyzing any topic that needs to be finalized. Using quantitative research methods for future cybersecurity workforce, this paper discusses the Future Cybersecurity Workforce, a problem statement, a purpose statement, research questions & matching hypotheses, a data collection plan, a data analysis plan, and a conclusion addressing legal and ethical issues.

KEYWORDS: Quantitative research, Cybersecurity, Cyber Performance

I. INTRODUCTION

The most efficient methods of evaluating research must be evaluated fundamentally. It will assist in understanding the real problems, analyzing them, and finding solutions. Qualitative research generates words rather than numbers for analysis as part of its goal, which is to understand some aspect of social life. Quantitative research methods aim to measure something, so qualitative approaches may appear unclear to those more familiar with quantitative methods [7]. The following topics will be discussed in this paper: using quantitative research methods on the Future Cybersecurity Workforce, Going Beyond Technical Skills for Successful Cyber Performance with a problem statement, purpose statement, research questions & matching hypotheses, data collection plan, data analysis plan, legal and ethical issues with a conclusion.

II. PROBLEM STATEMENT

The problem to be addressed in this study is identifying the lack of technical skills, domain-specific knowledge, and social intelligence for cyber education and the future of the cybersecurity workforce. Defining knowledge, technical skills, attributes, and other characteristics in the cyber domain is challenging due to its complexity. Developing cyber expertise and workforce through identifying gaps and arguing for the importance of a social fit is another challenging task. There is no quick fix for the complexity of the cybersecurity domain just by emphasizing soft skills instead of technical ones. The next challenge is optimizing cybersecurity workforces based on current and future demands and integrating them into a larger organization [6]. Identify the best method to continue cybersecurity research that produces fast, authoritative, and actionable results [5]. The lack of cyber security knowledge can result in significant losses for an organization and negatively impact its reputation in any industry. It will also affect the employee and the customer if all the personal information is not maintained or misused in any organization, especially in the banking or finance domain.

III. PURPOSE STATEMENT

The purpose of this quantitative research methodology is to identify the goal of the future Cybersecurity Workforce and how technical skills will be utilized to protect systems and digital data from cybercrime. It is necessary to create surveys & questionnaires that will provide the easiest & most effective method for understanding the gap and cyber security challenges. The purpose of the questionnaire is to identify the lack of technical skills, challenges, and

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 9, September 2024

|DOI: 10.15680/IJIRSET.2024.1309068|

communication gaps between organization, employees & customers, the lack of cyber security knowledge, and how the survey report and data analysis plan will help motivate and build a cybersecurity workforce [3]. Additionally, this article aims to provide some quick tips and solutions for protecting personal, financial, and confidential information [4]. It is also aimed at motivating & conducting security awareness sessions and knowledge of cybercrime and cyber threats, which are critical for businesses to remain digitally secure worldwide.

IV. RESEARCH QUESTIONS & MATCHING HYPOTHESES

The following research questions and hypotheses will guide the study based on the above study and methodology.

RQ1
What technical skills and domain-specific knowledge are required?

RQ2
What are the benefits of having a cybersecurity workforce?

RQ3
Developing a cyber security workforce is a challenge. What are some of those challenges?

Hypotheses

H10
A basic understanding of cybersecurity, including how to securely use technology and the internet.

H1a
A basic understanding of cybersecurity, including how not to use technology and the internet securely.

H20
To ensure that the organization's assets and personal information are protected.

H2a
To ensure that the organization's assets and personal information are not protected.

H30
Educate the team on cybersecurity and how to securely use the internet and technology.

H3a
Educate the team on cyber security, how to use the internet, and technology in an insecure manner.

V. DATA COLLECTION PLAN

The data will be collected by surveys and questionnaires as a part of a quantitative research method. In an organization or university, a representative group will administer a survey, followed by a short report discussing data analysis techniques with the participants. Participants may complete the survey in 15 minutes on average. The questionnaire will include questions about cyber security knowledge, a data protection plan, the use of technology with intelligence, and the future demand for technology with automation [1]. Participants will be provided a brief overview of the survey format before they begin. The survey includes a multiple-choice part (mandatory) and a comment part (optional). During the first part of the survey, participants will be prompted to provide personal details such as name, email address, phone number, gender, age, living situation, highest level of education, and job details. A second part of the survey will focus on identifying the security gap in the future cybersecurity workforce and user reactions to cybersecurity and technology-domain-specific concerns. After completing the data analysis plan, all personal information and survey reports will be securely deleted from the database.

VI. DATA ANALYSIS PLAN

The statistical package for social sciences (SPSS) tool will be used to analyze data for this research method. It describes the analysis and evaluation of the survey and report collected through qualitative research. Cybersecurity

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 9, September 2024

|DOI: 10.15680/IJIRSET.2024.1309068|

Workforce is a complex task, cognitively demanding, and often overwhelming for individuals and organizations alike. A survey report will confirm the next steps for cyber security workforce development. As a result, cyber security must be restructured at the process level, using new technologies and strategies to become more team-based, sharing the workload and information efficiently, and interacting effectively to mitigate security risks [2]. Since the cyber workforce will have access to sensitive data and little knowledge of their superiors and coworkers, they will need to engender trust with their superiors and coworkers. Technology changes rapidly, so the future cyber workforce may operate on outdated knowledge shortly after graduating. There must be more cyber security awareness sessions in universities and organizations, and everyone related to the future cyber security workforce must be encouraged.

VII. LEGAL AND ETHICAL ISSUES

An ethical code of conduct is necessary to conduct cyber security research. Cybersecurity is difficult to understand, so developing a moral code is essential [6]. The research model may raise legal and ethical issues because personal data (e.g., date of birth, email address, phone number, etc.) will be collected during the surveys and questionnaires. The early research phase requires the development of several strategies to resolve ethical tensions and issues in the areas of privacy and confidentiality. To avoid internal and external threats, conducting the survey and questionnaires anonymously for all participants is recommended.

VIII. CONCLUSION

This paper discussed the following topics: using quantitative research methods on the Future Cybersecurity Workforce, Going Beyond Technical Skills for Successful Cyber Performance with a problem statement, purpose statement, research questions & matching hypotheses, data collection plan, data analysis plan, and legal and ethical issues. Data quality plays a crucial role in quantitative research methods. Statistical calculations will be wrong or inferior if the data are not quality. In this paper, quantitative research is considered a possible research methodology, and the features of this type of research are evaluated regarding whether they meet the criteria needed for investigating technology-related concerns [7].

REFERENCES

1. Caulkins, B.D., Urquiola, K.B., Bockelman, P., & Leis, R. (). Cyber workforce development using a behavioral cybersecurity paradigm. IEEE. https://doi.org/10.1109/CYCONUS.2016.7836614
2. Champion, M.A., Rajivan, P., Cooke, N.J., & Jariwala, S. (2012). Team-based cyber defense analysis. IEEE. https://doi.org/10.1109/CogSIMA.2012.6188386
3. Chen, L.C., & Cotoranu, A. (2013). Enhancing the Interdisciplinary Curriculum in Cybersecurity by Engaging High-Impact Educational Practices. https://digitalcommons.pace.edu/cgi/viewcontent.cgi?article=1091&context=cornerstone3
4. Choo, K.K.R. (2011). The cyber threat landscape: Challenges and future research directions. 30(8), 719-731. https://doi.org/10.1016/j.cose.2011.08.004
5. Dark, M., Bishop, M., Linger, R.,& Goldrich, L. (2015). Realism in Teaching Cybersecurity Research: The Agile Research Process. Information Security Education Across the Curriculum. 453. https://doi.org/10.1007/978-3-319-18500-2_1
6. Dawson, J., & Thomson, R. (2018). The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance. https://doi.org/10.3389/fpsyg.2018.00744
7. McCusker, K., & Gunaydin, S. (2015). Research using qualitative, quantitative, or mixed methods and choice-based research. Perfusion, 30(7), 537-542. https://doi.org/10.1177/0267659114559116

BIOGRAPHY

Nabanita Das is a Senior Software Engineer and Integration Consultant. She has over 16 years of work experience with Middleware webMethods, Cloud Microsoft Azure & AWS, and domain- Healthcare, Banking, Insurance, Retail, Rx, HR, Finance, and Cyber security. She has in-depth knowledge of Integration, APIs, Security, Governance, and API standards. She is responsible for designing and developing integration solutions to support API and batch file transfer between various internal/external applications & partners. She has successfully delivered several complex projects with high accuracy & efficiency, resulting in significant cost savings & improved business processes with an exceptional

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 9, September 2024

|DOI: 10.15680/IJIRSET.2024.1309068|

team player, possessing outstanding technical & analytical skills, commitment, a positive attitude, selfless assistance, and excellent contributor. Her active participation in analysis and brainstorming solutions to fix defects and build them without compromising quality is commendable. She has excellent interpersonal skills and has consistently built strong relationships with stakeholders and clients. She persistently shares her views of project risks and provides solutions to address issues with conflicting priorities in high-pressure situations. She holds a Bachelor's degree in Computer Science & Engineering and an MBA in Project Management. Currently pursuing a Ph.D. in Computer Science from the National University. Her research interests are AI, Cyber Security, Integration, and Cloud computing.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details