**Safeguarding Against Modern Risks: A Guide to Cyber Resilience**

Abdulrahman Gamil Mohammed Ahmed

TP071012@mail.apu.edu.my

‌**1. Introduction**

In today's digital world, with looming cyber threats and organizations operating in a landscape full of risks, ‎cybersecurity awareness is emerging as a cornerstone of effective defense strategies. This research has an agenda to ‎inspect the subtle interplay between employee behavior and cybersecurity practices within organizational settings.‎ This study aims to unravel underlying factors of shaping employee attitudes and actions toward ‎cybersecurity based on individual behavior, organizational culture, and technological factors in order to ‎provide insights that can support the design of tailored interventions and policies toward development of a ‎cybersecurity mindful culture within organizations. The research conducted in this study, by mean of a combination of qualitative and quantitative ‎research methods, seeks to contribute to an advancement of knowledge on cybersecurity awareness and ‎behavior to empower organizations in increasing their cyber defense capabilities.

**2. Literature Review**

**2.1 Research Domains**

**2.1.1 Risk Management**: Cybersecurity, on the other hand, is a diverse area that comprises different areas of study, which help make the security measures effective and be able to grasp the general topic. One such area of study is Risk Management, it primarily works on identifying, analyzing, and prioritizing risks to minimize the impact of cyber-attacks. Researchers develop models and frameworks through which vulnerability in systems can be examined and the potential consequences from different types of cyber-attack scenarios can be evaluated. This will involve developing the plans for mitigation, threat modeling, and the evaluations of risks quantitatively (Atle Refsdal et al., 2015).‎

**2.1.2 Incident response** is the other vital area that deals with the identification, assessment, containment, and rehabilitation of cybersecurity events. Research into this field is performed on best practices for incident response teams, the effectiveness of different response tactics, and automated systems to take into account quick action. Another domain within this area is the forensic study of cyber events, which allows for the identification of the modes used for attack and ways to bolster defenses for the future (Naseer et al., 2021).‎

**2.1.3 Data Privacy and Protection:** It is an important discipline that provides solutions to safeguard sensitive and personal information. This includes policies for processing and storing data, access control systems, and techniques in encryption. Researchers focus on building technologies and standards to ensure confidentiality, integrity, and availability in any condition, even under advanced cyber-attacks. With a changing landscape of data privacy laws, such as the California Consumer Privacy Act (CCPA) and General Data Protection Regulation (GDPR), research in this area is also very much influenced (*Handbook of Research on Cyber Law, Data Protection, and Privacy*, 2022).‎

**2.1.4 Proactive cybersecurity measures** refer to the development of protections to secure systems before an attack occurs. Among its several studies are in the domains of intrusion detection systems, network security, and secure software development techniques. The primary objective is to be able to build strong defenses that could prevent attacks from causing damage. Techniques that employ artificial intelligence along with machine learning, to analyze patterns and abnormalities within network data, are being used to prevent cyber threatening (Abdi et al., 2024).‎

**2.1.5 Human Factors** is another critical input into cybersecurity. This refers to how people's behavior leads to breaches in security. Studies in this area include those on the psychology of phishing attacks, user awareness and training, along with studies on approachable security solutions. Researchers aim to understand how human mistakes manifest as security issues and try to develop countermeasures (Bowen et al., 2011).

**2.1.6 Multidisciplinary Approaches** domain focuses on how knowledge of different disciplines can be combined to address concerns, such as those in international relations, computer science, sociology, and law. Tackling the sophisticated and interconnected nature of cybersecurity threats requires a multidisciplinary approach. For instance, legal scholarship might influence the development and drafting of international cybersecurity norms and laws, and knowledge of the geopolitical context within which cyber threats arise can enhance national security blueprints (Berki et al., 2018).‎

The highlighted fields in cybersecurity combine several interrelated fields, each with huge viewpoints and progress in ensuring better protection of digitally stored resources. Researchers and practitioners can develop coherent and adaptive solutions to address emerging threats by considering input information from these vast domains.‎

**2.2 Similar Systems**

To understand and enhance cybersecurity protocols, analysis of similar systems and frameworks developed and implemented in other fields is important. These systems provide a wealth of information in and around practical strategies and possible pitfalls in cybersecurity procedures.‎

**2.2.1 NIST Cybersecurity Framework (CSF)**: A striking driving example here is the NIST Cybersecurity Framework (CSF) constructed by the American National Institute of Standards and Technology. The NIST CSF provides an expansive set of guidelines on how to manage and reduce cybersecurity risk. It is commonly used across various industries because of its ability to adapt and scale. There are five key functions of the framework: Identify, Protect, Detect, Respond, and Recover. To provide more specific actions and results, the function is further divided into categories and subcategories. Through the advocacy of a risk-based approach, the NIST CSF enables organizations to prioritize cybersecurity actions according to their specific risk and operational needs (Almuhammadi & Alsaleh, 2017).‎

**2.2.2 ISOIEC 27001** is an international standard designed for information security management systems (ISMS). It has a meticulous approach to information management for the attainment of confidentiality, integrity, and availability of sensitive company information. Best practices and controls that help develop, implement, manage, and maintain an ISMS and strive for its augmentation are stipulated in the standard. Companies that become certified by ISOIEC 27001 demonstrate strong commitment to information security practices, this can increase their credibility and reliability in the eyes of business partners and customers (*Implementing the ISO/IEC 27001:2013 ISMS Standard*, 2016).‎

**2.2.3 CIS Controls** formerly known as the SANS Top 20 is a leading framework that gives a prioritized list of steps to protect data and organizations from cyber-attacks. These measures were created by the Center for Internet Security with data from actual attacks. The three types of CIS controls—Basic, Foundational, and Organizational—each with specialized measures meant to reduce the most common and detrimental cyberthreats. Organizations looking for an understandable and practical plan to improve their cybersecurity posture will find this approach very helpful (Bashofi & Salman, 2022).‎

**2.2.4 Health Information Trust Alliance (HITRUST) CSF** is widely used in the healthcare sector to manage risks and protect personal patient information. The HITRUST CSF provides a comprehensive framework for risk management and protection of personal patient information through a centralized integration of various standards and regulations, including HIPAA, ISOIEC 27001, and NIST CSF. This framework is aimed at addressing specific risks and threats of health information systems and electronic health record systems, respectively, in line with the specific requirements of the healthcare industry (*Health Care Cyber Security Professionals’ Perceptions Regarding the Implementation of a Quantitative Risk Management Framework - ProQuest*, 2022).‎

**2.2.5 Cybersecurity Capability Maturity Model (C2M2)** Another key tool for the examination and strengthening of an organization's cybersecurity ability is the Cybersecurity Capability Maturity Model (C2M2). C2M2, developed by the U.S. Department of Energy, is a maturity model that enterprises can use to assess their current cybersecurity processes and identify areas where enhancement is needed. Ten domains, including incident response, threat and vulnerability management, and asset management, are addressed in the model. Organizations can develop a roadmap to enhancement of their cybersecurity resiliency and maturity by following C2M2 (Ghaffari & Abouzar Arabsorkhi, 2018).‎

Strong cybersecurity planning can be developed by examining these comparable systems for best practices and recurring themes. It will be composed of a base of a risk-based strategy, the combination of many rules and regulations, and focus on developing continuously.

**3. Research Methodology**

**3.1 Identify Target User**

In this section, we delve deeper into the methods and strategies we are going to use to identify the target user population for our research regarding employees' cybersecurity awareness and activity within an organization. Understanding the characteristics and nature of our target population is essential for developing effective measures and stratagems for strengthening cybersecurity provisions. To this end, in this research study, we will use qualitative and quantitative methods to locate and recruit participants.

‎**3.1.1 Organisational Partnerships**: A key aspect of our recruitment strategy will be ‎to establish strong partnerships with an array of organizations. We will engage a broad ‎spectrum of employees representing varied sectors and industries by partnering with ‎IT departments, HR departments, and corporate leaders. These partnerships will render the ‎recruitment process more efficient and the generalization of our research findings more ‎valid.‎

**‎- Networking and Outreach:** We plan to reach out to the companies willing to ‎participate within our study through industry conferences, online discussion boards, and ‎professional networking sites. We will reach out to them through focused outreach ‎campaigns to foster a mutual relationship, where they provide us access to their ‎employees for our research needs (Singh et al., 2017).

**‎-Key Stakeholder Engagement:** Engaging the key stakeholders of the partner ‎organizations, such as senior management, IT security teams, and employees' ‎representatives, will be key in gaining their support and permission, who may be involved at the beginning of the research cycle to ensure organizational ‎alignment with the study's aims and objectives (Bourne, 2016).‎

**‎ 3.1.2 Random Sampling Techniques**: We'll employ random sampling techniques to select ‎our participants from within the organization to ensure minimal selection bias and optimal ‎representativeness. To ensure that every individual of the population has an equal likelihood of getting ‎included in the sample, random sampling involves selecting people randomly from the ‎population, without using any criteria to make the selection. ‎

‎-**Random Selection of Participants:** We'll randomly select participants from each ‎participating organization to ensure diversity is included in our sample. The participants will ‎belong to diverse departments, job roles, and hierarchical positions. This captures a variety of ‎perspectives and experiences in relation to cybersecurity awareness and behavior.‎ ‎

**‎-Sampling Frames:** We will develop lists of personnel from each organization who ‎meet the eligibility criteria of the research, or sampling frames, to ‎allow random sampling. These sample frames, which shall be used only as a ‎reference of choosing the respondents through random sampling procedures, shall ‎be made on relevant criteria such as job description, department, and length of employment.‎

‎**3.1.3 Demographic Criteria and Stratification**: To ensure ample diversity and ‎representation from among the target population, we will apply demographic criteria on top of ‎random sampling. Through this stratification, we may consider population ‎heterogeneity and explore how cybersecurity knowledge and practice differ between ‎different demographic groups, including age, gender, education, and work ‎characteristics of the participants (Yee Guan Yap et al., 2008).‎

**‎- Demographic Definition:** A careful consideration of the related variables, such as ones that can impact either ‎knowledge or behavior in cybersecurity of people, including, but not limited to, age status, job ‎position as management, IT personnel or others, frontline employees, and level of technical competence.‎‎

**‎ - Proportionate Representation:** To ensure that all the sub-groups are represented fairly in ‎the sample, we aim to create proportionate representation within all the demographic strata. ‎Through this, biases can be minimized, and better comparisons and analyses can be made ‎between various sub-groups in the demographics.‎

‎**3.1.4 Informed Consent and Confidentiality of Participants**: Prior to recruitment of volunteers into the study, we ‎will obtain informed consent from all the individuals, confirming all of them are aware of the ‎purpose of the study, their rights as participants, and whether it serves them any harm or ‎benefits. The study's overall purpose, the procedures for locating data, the steps ‎taken by the researcher to ensure the anonymity of the participants, all shall be outlined in the ‎informed consent forms

**‎-Ethical Considerations:** In all cases of human subjects' research, we will follow ethical standards ‎and principles, which incorporate the principles of informed consent, the right to self-determination, ‎guarantees of privacy, confidentiality, and data anonymity. Before the commencement of data collection, ‎relevant institutional review boards or ethics committees will grant their ethical approval.‎ ‎

**‎-Privacy and Confidentiality:** As a means to secure the privacy and confidentiality of participants, any data ‎collected from participants will be coded and securely stored. Study data and personally identifying ‎information will not be linked. Only de- or re-identified data will be used for reporting and analysis ‎purposes.‎

‎

By employing these tools and methods to reach the target audience, we aim to create a collective and more ‎representative sample of employees from different organizations, industries, and class groups. From this, ‎we will be in a position to assess critical information about the employee cybersecurity knowledge and ‎practices, and will allow us to develop further interventions and policies that will enhance the state of ‎cybersecurity in an organization (*Merriam-Webster Dictionary*, 2024).‎ ‎

**3.2 Sampling Method**

We describe in more detail the sampling methodology that we applied in our first sub-study with regard to employees' awareness and behaviors toward organizational cybersecurity and how such employees' characteristics affect the level of susceptibility to phishing. The design of the study is usually dependent on sampling, which determines the extent to which the findings can be generalized or applied in the general public. A combination of the convenience and stratified random sample methods will ensure that the participants recruited are both pragmatic and representative.‎

‎**3.2.1 Stratified Random Sampling:** The part of the population concerned is stratified into separate ‎‎subsets or strata using relevant characteristics or attributes, such as organisational characteristics, ‎‎qualities, cybersecurity awareness level, or demographic qualities. Once the strata have been defined, ‎‎participants are selected randomly into each stratum, thus ensuring a uniform representation of ‎‎cross-sections under the respective categories.‎ ‎

**- Identification of Strata:** We will identify important strata using factors like either job ‎functional, departmental, or organisational tenure as well as previous cyber training or ‎experience that, according to the researchers, help in determining a person's awareness and ‎behaviour towards cybersecurity (Burgess, 2016).‎

‎

‎ - **Proportional Allocation:** We will delineate the appropriate sample size for each stratum based ‎‎on the relative proportion of the population from which the different stratum has been identified ‎to represent larger and more significant stratum to the samples, thus ensuring meaningful. ‎‎comparisons can be made between respective categories or groupings.‎

‎

‎ - **Random Selection within Strata:** This will be ensured through computerised sample or ‎random number generation. Random selection reduces selection bias and fairly gives every ‎person in the population an equal probability of becoming

‎**3.2.2 Convenience Sampling**: Besides stratified random sampling, we shall also include ‎convenience sampling to ease the process of participant selection, particularly in research ‎environments where access is constrained, as well as in situations where various organizations ‎or groups may not be willing to provide data or information.‎

**‎- Access to Specific Organizations:** Convenience sampling will allow us to access data and ‎‎information from organizations that would otherwise be hard to reach or those that are ‎conveniently available. Besides, convenience sampling will also enable us to have access to ‎numerous organizations and participants within a short period, even though this approach is ‎likely to provide some sampling bias.‎ ‎

**‎- recruiting methods:** To contact potential participants and encourage them to take part in the study, we will use various recruiting methods, such as email invites, social media sites, online surveys, and professional networks. All these hiring approaches will be tailor-made based on special characteristics and the nature of each potential target market (Scholarios & Lockyer, 1999).‎

**3.2.3 Sample Size Determination**: Selecting an appropriate sample size is important in ensuring that the power of a statistical test and reliability in the study results is guaranteed. The appropriate sample size will be determined while considering many aspects, among them being the expected effect size, the level of accuracy required, and the threshold of statistical significance.‎

**- Power Analysis:** Power analysis will be carried out to estimate the smallest sample size needed to find significant differences or correlations between variables that are known with a given confidence and power. Through this technique, it will be possible to ensure the sample size is sufficient to achieve the objectives of the study and to detect any significant relationships or effects.‎

**3.3 Quantitative Data Collection Method**

Surveys are a key quantitative data collection channel in the study. Structured questionnaires will be developed to investigate employee attitudes, knowledge, and behavior towards cybersecurity within organizations. The survey will investigate and thus cover questions ranging from cyber threat awareness, adherence to currently provided security protocols within the organization, the frequency of incidents related to security, and support from the organization based on the employees' perception of cybersecurity.

The surveys will be administered electronically through online survey platforms, making it a very efficient method with which to collect data. The use of standardized questionnaires means that similar data is collected across different organizational settings, facilitating comparisons and generalization (Couper, 2016).

With the nature of the survey being quantitative, the data collected are amenable to statistical procedures in order to provide an understanding of general trends in employee behavior regarding cybersecurity. The data collected using the surveys, from the identification of any potential vulnerabilities to a comparison of the performance of the security systems in place, act as a quantitative eye for scanning the cybersecurity pool in organizations (Couper, 2016).

Full ethical procedures, such as consent to participate, are followed during the surveying process. The issue of data confidentiality is also ensured by the research team, thus upholding participant rights.

**4. Conclusion**

In conclusion, this research has shed light on the complex dynamics of employee behavior ‎and its implications for cybersecurity within organizations. This is valuable, as the factors that ‎influence employee attitudes, perceptions, and actions toward cybersecurity will be assessed to ‎influence the development of effective programs and policies. From the importance of ‎organizational culture to the role of individual motivations, our findings underscore the ‎multifaceted nature of cybersecurity awareness and the need for holistic approaches to fostering ‎cyber hygiene. As organizations are dealing with an emerging complex threat landscape, ‎insights that this research shall provide can be guiding light, energizing organizations to create ‎a culture in building cybersecurity resilience from within. Investing in people-focused ‎cybersecurity empowers organizations to build up their defenses against attacks, thus mitigating ‎risks and securing against the looming face of a cyber-attack.‎

**5, References**

* Atle Refsdal, Bjørnar Solhaug, & Ketil Stølen. (2015). Cyber-risk Management. SpringerBriefs in Computer Science, 33–47. <https://doi.org/10.1007/978-3-319-23570-7_5>
* Naseer, H., Maynard, S. B., & Desouza, K. C. (2021). Demystifying analytical information processing capability: The case of cybersecurity incident response. Decision Support Systems, 143, 113476–113476. https://doi.org/10.1016/j.dss.2020.113476

‌

* Handbook of Research on Cyber Law, Data Protection, and Privacy. (2022). Google Books. https://books.google.com.my/books?hl=ar&lr=&id=BRBoEAAAQBAJ&oi=fnd&pg=PR1&dq=Data+Privacy+and+Protection%E2%80%8E+cyber&ots=Ri5Ow5ZLtM&sig=cOg-Nf0gFAiLCuBi0GEBT1uNNIQ&redir\_esc=y#v=onepage&q=Data%20Privacy%20and%20Protection%E2%80%8E%20cyber&f=false

‌

* Abdi, N., Abdullatif Albaseer, & Abdallah, M. (2024). The Role of Deep Learning in Advancing Proactive Cybersecurity Measures for Smart Grid Networks: A Survey. IEEE Internet of Things Journal, 1–1. https://doi.org/10.1109/jiot.2024.3354045

‌

* Bowen, B. M., Devarajan, R., & Stolfo, S. (2011). Measuring the human factor of cyber security. Columbia Academic Commons (Columbia University). https://doi.org/10.1109/ths.2011.6107876

‌

* Berki, E., Juri Valtanen, Chaudhary, S., & Li, L. (2018). The Need for Multi-Disciplinary Approaches and Multi-Level Knowledge for Cybersecurity Professionals. Advances in Information Security, Privacy, and Ethics Book Series, 72–94. https://doi.org/10.4018/978-1-5225-5297-0.ch005

‌

* Almuhammadi, S., & Alsaleh, M. (2017). Information Security Maturity Model for Nist Cyber Security Framework. Computer Science & Information Technology (CS & IT). https://doi.org/10.5121/csit.2017.70305

‌

* Implementing the ISO/IEC 27001:2013 ISMS Standard. (2016). Google Books. https://books.google.com.my/books?hl=ar&lr=&id=Yy6pCwAAQBAJ&oi=fnd&pg=PR6&dq=ISO+IEC+27001%E2%80%8E&ots=vsr48hd8SR&sig=UYkh9-OHyZvaxKTaoXLunpiiXIQ&redir\_esc=y#v=onepage&q=ISO%20IEC%2027001%E2%80%8E&f=false

‌

* Bashofi, I., & Salman, M. (2022). Cybersecurity Maturity Assessment Design Using NISTCSF, CIS CONTROLS v8 and ISO/IEC 27002. https://doi.org/10.1109/cyberneticscom55287.2022.9865640

‌

* Health Care Cyber Security Professionals’ Perceptions regarding the Implementation of a Quantitative Risk Management Framework - ProQuest. (2022). Proquest.com. https://www.proquest.com/openview/c90b3ed2923ca9bf4fc42b8888831cc4/1?pq-origsite=gscholar&cbl=18750&diss=y

‌

* Ghaffari, F., & Abouzar Arabsorkhi. (2018). A New Adaptive Cyber-security Capability Maturity Model. https://doi.org/10.1109/istel.2018.8661018

‌

* Singh, A., Jenkins, C., B Calys-Tagoe, Arulogun, O. S., Sarfo, S., B Ovbiagele, A Akpalu, S Melikam, E Uvere, & Owolabi, M. O. (2017). Stroke Investigative Research and Education Network: Public Outreach and Engagement. Journal of Community Medicine & Health Education, 07(02). https://doi.org/10.4172/2161-0711.1000518

‌

* Bourne, L. (2016). Targeted Communication: The Key to Effective Stakeholder Engagement. Procedia: Social & Behavioral Sciences, 226, 431–438. https://doi.org/10.1016/j.sbspro.2016.06.208

‌

* Yee Guan Yap, Duong, T., Bland, M., Malik, M., Torp-Pedersen, C., Lars Køber, Connolly, S. J., Gallagher, M. M., & A. John Camm. (2008). Potential demographic and baselines variables for risk stratification of high-risk post-myocardial infarction patients in the era of implantable cardioverter-defibrillator — A prognostic indicator. International Journal of Cardiology, 126(1), 101–107. https://doi.org/10.1016/j.ijcard.2007.03.122

‌

* Merriam-Webster Dictionary. (2024, June 8). Merriam-Webster.com. https://www.merriam-webster.com/dictionary/demographic

‌

* Burgess, P. (2016, March). Identifying Ordered Strata: Evidence, Methods, and Meaning. ResearchGate; Society for Sedimentary Geology. https://www.researchgate.net/publication/297721347\_Identifying\_Ordered\_Strata\_Evidence\_Methods\_and\_Meaning

‌

* Scholarios, D., & Lockyer, C. (1999). Recruiting and Selecting Professionals: Context, Qualities and Methods. International Journal of Selection and Assessment, 7(3), 142–156. https://doi.org/10.1111/1468-2389.00114

‌

* Couper, M. P. (2016). Technology Trends in Survey Data Collection - Mick P. Couper, 2005. Social Science Computer Review. https://journals.sagepub.com/doi/abs/10.1177/0894439305278972?casa\_token=WXAS56dh0YUAAAAA:85N6sKAZ1aUHFxskMH0ev7JgDbDUpQh\_tWKLzuE8vLU7b8JHejVwChvAvcUXM2c8xmDVWLNEtVw1\_A

‌