**Topic: Does Security Awareness Training Make Any Measurable Difference**

**Table of Contents**

[1. Introduction 4](#_Toc173149843)

[1.1 Background to the problem 4](#_Toc173149844)

[1.2 Justification for the research 6](#_Toc173149845)

[2. Research definition 7](#_Toc173149846)

[2.1 The practical problem 7](#_Toc173149847)

[2.2 Existing relevant knowledge/Literature review 7](#_Toc173149848)

[2.2.1 Current existing cyber security training programs adopted by organizations 7](#_Toc173149849)

[2.2.2 Case studies 8](#_Toc173149850)

[2.2.1 Case study 1: SANS institute 8](#_Toc173149851)

[2.2.2 Case study 2: Xerox Corporation 10](#_Toc173149852)

[2.2.3 Case study 3: University of California, Berkeley 11](#_Toc173149853)

[2.2.4 Case study 4: Maersk 12](#_Toc173149854)

[2.3 Aim 14](#_Toc173149855)

[3. Methodology 15](#_Toc173149856)

[3.1 Methods and techniques selected 15](#_Toc173149857)

[3.2 Data collection methods 15](#_Toc173149858)

[3.2.1 Qualitative research methods 15](#_Toc173149859)

[3.2.2 Qualitative data collection methods 16](#_Toc173149860)

[3.3 Online interactive procedure 17](#_Toc173149861)

[3.4 Justification of mixed research methodology 19](#_Toc173149862)

[3.3 Research procedures 19](#_Toc173149863)

[3 Planning and scheduling 20](#_Toc173149864)

[4 Progress to date 20](#_Toc173149865)

[References 21](#_Toc173149866)

[Appendix 23](#_Toc173149867)

[Sample Questionnaire 23](#_Toc173149868)

# **Introduction**

## **1.1 Background to the problem**

In the current digital age, cyber-security threats have proliferated and has presented a significant challenge to many organizations across all the sectors. Cyberattacks ranging from insider threats, phishing scams pose a security risks to the organization integrity, confidentiality, and available of sensitive data and the critical systems. As companies increasingly rely on digital techn0ologies to store vast amounts of data and conduct their daily operations, the impact of cyber incidents on organizations’ operations, reputation and financial stability cannot be overstated.

Amidst, the cyber evolving threats and landscape, workers represent both a critical line of defense and one of the potential vulnerabilities in the security posture of the organization. While technological solutions like intrusion detection systems, anti-virus, and firewalls have been continuously used and plays an important role, human negligence and error remains one of the significant contributors to security breaches. The 2023 Verizon data breach report showcased that 82 percent of security and data breaches involved a human element. This includes incidents in which employees and workers expose data and information directly to hackers by either making a mistake when carrying out their activities or by knowingly submitting information to hackers. The report went to state some of the 2023 common errors which were done and which resulted to cyber-attack. One type of error was what Verizon referred to as skilled error which occurs due to phishing scams. The second type of error was related to decision making and which occurred when a worker comprises sensitive risks because their do not understand the risk involved. Verizon attributed 73 percent cyberattacks as a result of human element (Verizon, 2023).

According to IBM report of 2011, the cost of human error can result to huge cost. Some of the cost is related to scam cost which can cost organizations to about $5 per every record stolen. As a result, about fifty-one percent of organizations worldwide are planning to invest in security awareness and to include test, employee training, and threat detection (IBM, 2021).

From the two major reports it is evident that substantial proportion of cyber security incidents are attributed to human factors which includes falling victims to phishing attacks, clicking of malicious links, and mishandling of sensitive information. As stated some organizations have already implemented security awareness training programs as advised by IBM. These training programs are aimed at educating workers about the current common threats and promoting some of the best cyber security practices. Some of these initiatives usually include online modules, simulated phishing exercise, interactive workshops, and informational campaigns all which are designed to equip employees with skills and knowledge to mitigate and recognize potential security risks.

Despite these widespread and recommendations of security awareness training programs to cybersecurity threats, questions still remain on the effectiveness of awareness programs in achieving tangible improvements in security outcomes. While anecdotal evidence, recommendations, and case studies suggests and a well-designed training program usually leads to positive changes in worker’s behavior and reduction of cyber threats by over 30 percent, there is limited research on security awareness programs. Moreover, measuring the impact or the influence of security awareness training programs in terms of the measurable outcomes like improved response times, a reduced incident rates, and an enhanced organizational security posture presents a methodological issue.

Against this gap and backdrop, there is a need to have a comprehensive research to evaluate the efficacy or efficiency of security awareness training programs and assess whether the process makes any measurable difference in the security posture of an organization. By examining the relationship between key cybersecurity metrics like employee awareness and incident rates and security awareness training can go a long way to highlighting and providing valuable insights into the limitations and strengthens that security awareness training offers to making organization assets secure. Also, this enhances organizations resilience against the current evolving cyber threats and ensuring that an investment in cybersecurity training among organizations. Also it helps in identifying areas of improvement and empowers workers to become active participants in the defense of IT assets to reduce the likelihood of the current costly security breach.

## **1.2 Justification for the research**

In the current existing research on security awareness and training, most of them rely on what one can refer to as anecdotal evidence or what others refer to as theoretical framework rather than empirical data. This research fills this gap by conducting a comprehensive empirical research to assess the effectiveness of the current cyber security awareness.

Second most organizations usually struggle to implement and design effective security awareness program. This is so because there is lack of practical guidance and evidence-based strategies. This research closes this gap by developing a sample interactive procedure based on the findings of the research, this in turn provides companies and organizations with actionable recommendations for optimizing the various training initiatives

# **2. Research definition**

## **2.1 The practical problem**

In this case the practical issue is a security awareness training program which is to be used to mitigate cybersecurity threats. The practical issue revolves around determining whether the training programs make a tangible difference in enhancing workers security behaviors and at the same time reducing the security incidents.

The key issues in this case are workers’ retention and engagement. This is ensuring that workers are engaged with the cyber security training content and at the same retaining the information in the long term. Second, is translating the gained knowledge from training into a secure and consistent behavior. Third is deploying a reliable method and metric to measure the impact of the training program. Lastly is keeping the training program relevant amidst the current evolving cybersecurity threats and the high workers’ turnover.

## **2.2 Existing relevant knowledge/Literature review**

### **2.2.1 Current existing cyber security training programs adopted by organizations**

According to the cyber security magazine, cyber security global crime is expected to grow by 15 percent in the next three years. Cyber security and cybercrime are one of the new entrants into the top ten of the most severe global risks over the last ten years. It is due to this that most organizations have adopted various trainings programs to enhance their defense and techniques against cyber threats and at the same time improve workers’ awareness (ESET, 2021). Most organizations have adopted various training programs; one of the widely adopted program by organizations is the Certified Information Systems Security Professionals. This is a certification which has been adopted by organizations and a requirement for all the security practitioners, and IT managers. From the training awareness programs, the workers gain diverse set of skills in this case. These includes the principles of the security in this case the CIA principles. Second is the security governance, risk management, and compliance. Also, from the program workers gain all the business, regulatory, and legal requirements for cybersecurity. Other forms of knowledge gained include the cybersecurity models, cyber security design frameworks and principles.

Some example of organizations which have already adopted this training program are the big companies like Microsoft, Google, and IBM. In here the organizations require their employees to obtain the cyber security program to ensure that their team have a strong foundation in security practices and principles.

Certified Ethical Hacker is another security program which has been widely adopted by most organizations. The program is offered by the EC-Council. The awareness mainly focusses on practicing and understanding the hacking techniques to identify some of weaknesses that exists in one systems. Also in here the employees are training in CompTIA Security; which covers the principles of network security and management of risks (EC-COUNCIL, 2022).

However, these training programs are said to have gaps. For example, in the CISSP program, employees rely mostly on theoretical knowledge rather than the current practical knowledge. This can result to inability to apply the knowledge in real-world scenarios. Second, is the current evolving nature of cyber threats. The current new attacks like exploiting IOT devices and taking advantage of AI to launch sophisticated attack are not covered in these programs.

### **2.2.2 Case studies**

### **2.2.1 Case study 1: SANS institute**

SANS Institute has collaborated with many organizations to develop security awareness training program that is tailored to company’s risk profile and their specific needs. It is important to note that SANS institute is one of the leading organizations in delivering and designing cybersecurity security training programs. The organization has collaborated with multinational corporation to develop a customized security awareness training program which was tailored to health risk profile and organization’s specific needs. The training covered various aspects like secure handling of information, recognizing insider threats indicators, and data protection policies (SANS INSTITUTE, 2021).

One of the example of the training programs developed by SANS institute is the knowledge areas assessment. According to SANS the training was meant for the subject matter expert. The program was meant to make the experts aware on several known security risks and identify the areas of improvement (SANS, 2021). The training program is located on the organizations site at <https://www.sans.org/security-awareness-training/products/cyber-risk-insight-suite/knowledge/> One of the major findings of the study is that security training of knowledge awareness is essential to subject matters as it prevents them from security related risks.

**Gaps in the case study**

Following the implementation of the security program provided by SANs institute, the multinational approach experienced a reduced number in insider threat reduction including data breaches, employees demonstrated an improved adherence to data procedures and policies. Most of the organizations culture evolved, with workers actively participating in adopting a shared responsibility and cybersecurity initiatives for protecting organizational assets.

However, while the SAN’s institute case study offers some valuable insights into the effectiveness of security awareness training programs, there are areas and gaps which can be pointed out. First, the case study does provide a specific quantitative metrics to measure the extent of improvement. This includes presenting concrete metrics like percentage decrease in successfully phishing attempts or reduction in incident response times.

Second, the case study highlights only on immediate outcomes following the implementation of security awareness programs. For example, the case study only points out reduction of security incidents as a result of cyber security awareness programs. The case study does not delve onto long term sustainability or even go ahead to assess the impact of its training program on broader organizational resilience against the various cyber threats. One can state that SANs security program of 2023 does not provide a more comprehensive evaluation on long-term and short-term outcomes which would provide a more nuances understanding of the training programs effectiveness.

Third while the training program mention improvements in employees’ awareness, it does not incorporate direct feedback by employees who participated in the security awareness program. Gathering workers’ perspective on the security training content, perceived effectiveness, delivery methods can provide valuable insights for refining future training initiatives and at the same time addressing any concerns or gaps.

Third the case study does not fully provide or explore the contextual factors which might influence the effectiveness of security awareness programing like employee demographics, organizational culture, or even industry specific issues. Understanding these factors and all their impact on security training program outcome is essential as it can provide tailoring training programs to meet the unique needs and issues of various organizations.

### **2.2.2 Case study 2: Xerox Corporation**

Second case study is the Xerox corporation, the company faced issues related to information security data breaches. As a result, the company decided to carry out a security awareness training program for all its employees. The security awareness program was aimed at educating employees about the various cybersecurity risks and promoting some of the best practices for safeguarding company sensitive information. The security training module included interactive modules, in-person workshops which were conducted by cybersecurity experts, and carrying out a simulated phishing exercises.

After carrying out the security awareness training program, Xerox reported a reduction in security incidents which were attributed to employee negligence like accidental data leaks. Second, is that employees demonstrated an improved awareness of social engineering tactics and phishing scams. This lead to a decrease in successful phishing attacks targeting the organization. Third is that the company incident response capability improved with workers reporting security incidents promptly (Xerox, 2019).

**Gaps in the case study**

Even though security training program by Xerox seems to be effective as reported by the company, there are few gaps with the case. First, just like the SANs institute case, it lacks specific quantitative measure the effectiveness of the training program. While the company mentioned a reduction in its security incidents which were attributed by workers’ negligence like accidental data leaks, Xerox does not provide what one can refer to as concrete data on the extent of this reduction.

Second is that the case study majorly focuses on immediate outcomes like decrease in phishing attempts. Just like the SANs institute case study it does not provide long term sustainability of these improvements. Third the case study does not provide the correlation between the training program and overall company resilience against cyber threats. According to… by providing both long term and short term outcomes, it provides insights into sustainability outcomes

### **2.2.3 Case study 3: University of California, Berkeley**

The third case study which can be highlighted is the University of California case study. The institution reported a continuous cybersecurity issues and data breaches affecting its students, staff, and faculty. As a result, the university decided to carry out a cyber-security awareness program targeting its students and staff. The training included online modules, awareness campaigns which were tailored to various audience groups, and in-person workshops.

After the training program, the university reported a decrease in cybersecurity incidents including phishing attempts, decrease in unauthorized access to university data and systems, decrease in phishing attacks. The incident response capabilities were enhanced and students demonstrated an improved cyber security best practices (University of California, n.d.).

**Case study gaps**

As highlighted above, the university cyber security awareness program was tailored towards the students and staff which resulted to decrease in authorized access to university systems and data. However, the case study lacks some quantitative metrics which can be used to measures the effectiveness of the program. Second while the case study mentions that there was a decrease in phishing attacks it does not provide concrete data on the extent of the malware reduction. Third, even though the case study primary focus is on immediate results like incident reduction. It doesn’t delve into long term sustainability. Lastly, even though the case study mentions that the training initiative targets the staff and students, it doesn’t detail on employee feedback or any engagement. Gathering direct feedback from the participants offers a more detailed insight into the effectiveness of the training content and delivery methods.

### **2.2.4 Case study 4: Maersk**

Another case study is the Maersk, cyber security awareness program which was conducted in 2017. Maersk is a global shipping company which was faced with cybersecurity incident where it feels a victim of NotPetya ransomware attack in 2017. This resulted to widespread disruption of company’s operations and financial losses.

In response to the attack, the company implemented a raft of measures one of them being carrying out a cyber-security training program to all its employees. The training focused on raising awareness of the various cybersecurity risks, enhancing incident response capabilities across the company, and promoting best practices (Maersk, n.d.).

Following implementation of cyber security awareness training program. The company reported a decrease in malware related attacks as workers become more informed so they were able to detect any suspicious attachments. Its response capabilities were strengthened with workers demonstrating an improved readiness. Lastly a culture of training initiatives and proactive measures was also reported.

**Gaps in the case study**

Even though the security awareness program at Maersk resulted to decrease in malware related attacks, several gaps were not addressed by the organization. First, the case study doesn’t provide specific data and information about the content of the training program. While the training focused on the awareness of various cyber security programs, the programs lacks specifics covered and the delivery methods used.

Second, even though the case study highlights some of the immediate outcomes of the training program in which it conducted, the training does not address some of the long term sustainability of these improvements. The awareness program does not mention of the ongoing efforts or measures which are taken to reinforce training concepts and sustain employee behavior over time.

Lastly while the case study mentions the fostering of organizational culture with Maersk, it does not provide an in-depth analysis and discussion of the Maersk’s culture surrounding cybersecurity before the implantation of the training program. According to… understanding pre-existing attitudes and culture towards cybersecurity with an organization can provide valuable context for the evaluation of the security awareness training awareness initiative.

## **2.3 Aim**

1. To examine and determine the extent to which security awareness training programs influences workers’ behaviors, attitudes, and knowledge related to cyber security
2. To identify some of the measurable metrics to assessing security awareness training effectiveness like improved response times, increase reporting of the suspicious activities, and reduction in security incidents
3. To provide actionable recommendations and insights for optimizing security awareness training programs based on empirical findings

Effectiveness of security training by Bulgurcu

One of the studies which have evaluated direct impact of security training on workers’ behavior is Bulgurcu, “Information Security Policy Compliance: An Empirical study of rationality-based beliefs and information security awareness”. The aim of the research by Bulgurcu was to understand the role of workers’ awareness in information security policies that influences their compliance behavior. Also, the author has investigated the relationship between workers’ rationality beliefs like beliefs about the outcome of not complying and complying. Lastly, the author has tested and developed a theoretical model which explains workers’ compliance intentions based on their rationality-based beliefs and awareness.

The framework developed by Bulgurcu was the theory of planned behavior commonly known as the TPB and the underlying theoretical framework for the study. The framework indicates that worker’s behavior is determined by intention to perform the said behavior. According to Bulgurcu it is determined by three major factors which are perceived behavior control, the subjective norms, and attitude towards the behavior. The individual negative or positive evaluation of performing the behavior. The perceived behavior control of a worker that perception of their ability to perform the said behavior. Lastly, the subjective norms are the perceived social pressure to perform the behavior not to perform or to perform.

Puhakainen security aware culture

Kruger and Kearney security awareness program

# **3. Methodology**

## **3.1 Methods and techniques selected**

Based on the gaps identified from the literature review, and the critiques which have been provided, mixed approach research methodology would in this case best suited for this study. The approach combines quantitative and qualitative methods to provide a comprehensive understanding of the research topic. Also, the methodology will assist in addressing the gaps identified from the previous studies.

The first phase for this study was to the quantitative phase. In here a survey questionnaire will be developed based validated measures and scales identified in the literature review. In this case, this measures would be security self-efficacy, perceived barriers, and what I can refer to as response efficacy. Also, in here the study utilizes what is known as stratified sampling technique; this will be used to ensure that there is a representation across various organizational sectors. The questionnaires will be administered to a large sample of workers to assess their cybersecurity awareness, behaviors, and attitude. Lastly, a statistical analysis will be used like Structural Equation Modelling (SEM) and regression analysis to examine the relationship between the various variables (Terrell, 2019).

## **3.2 Data collection methods**

### **3.2.1 Qualitative research methods**

One of the techniques which was utilized to collect data was survey. In here, surveys were administered to both after and before the security training programs. This was done to measure the changes in cybersecurity knowledge, self-reported behaviors, and attitudes. Before the training the survey was distributed to participants one week before the training and after three months after the training to access the long term impacts. The questions in this case were Likert based that is on a scale of 1 to 5 and multiple-choice based questions.

Surveys data collection method was implemented as it provided an efficient way to gather data from large number of participants. Also, it provided quantifiable data which can be used statistically to analyze or detect changes over a period of time. Both the pre and post training comparison can be used to highlight the effectiveness of training in changing attitudes and knowledge.

The second data collection method was the incident reports analysis. In here an analysis of security incidents reports from IT departments was done after and before the security awareness training program. The pre-training incident data was collected before the security training program and after six months, after the security awareness program. The metrics utilized in this case were the malware infections, unauthorized access attempts, incidents reported by employees, and phishing email click-throughs. This technique was used as it provided an objective and real-world data on security incidents. Also it provided a way to analyze incident trends before and after the training. This in turn revealed the trainings impacts on the actual security incidents practices.

### **3.2.2 Qualitative data collection methods**

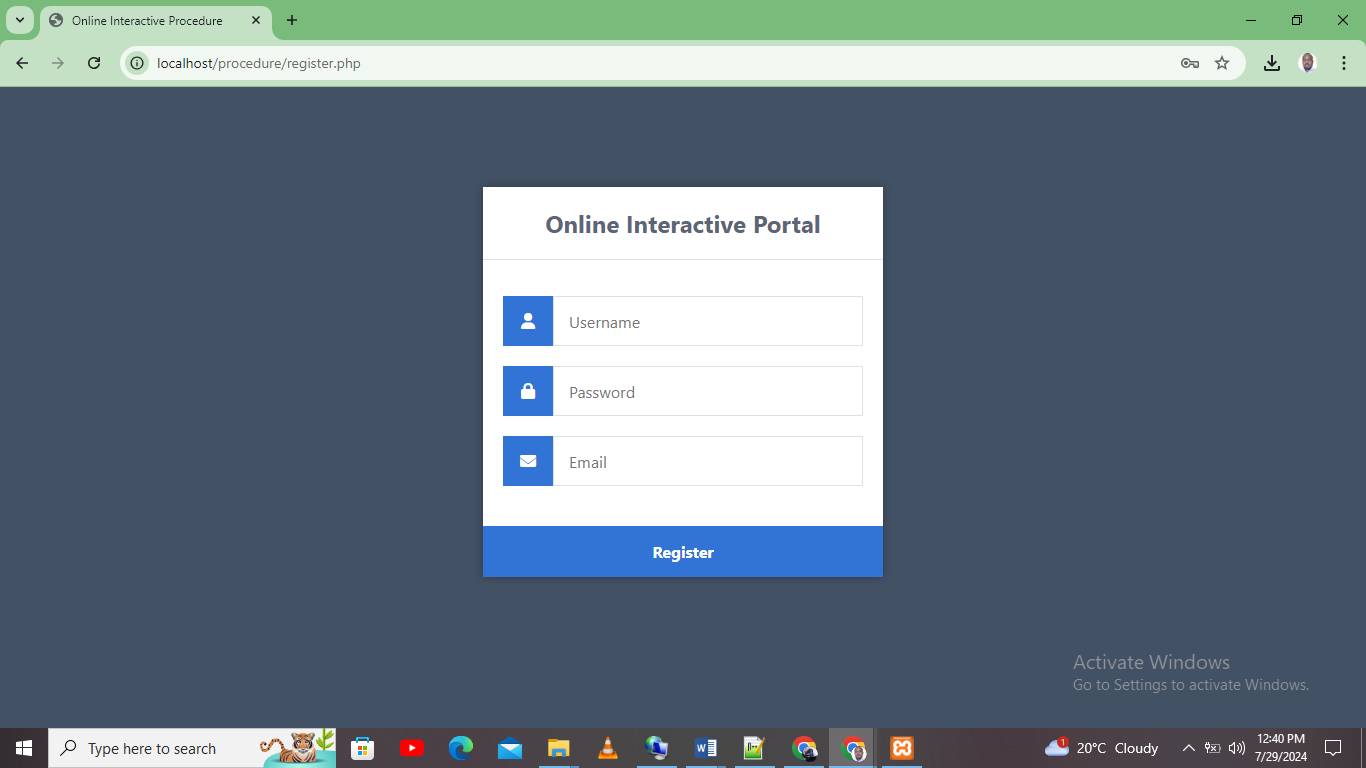
One of the technique which was utilized in this case was the semi-structured interviews with workers to gather an in-depth insight into the perspective of the security program effectiveness. The selection of the participants in this case was based on departments and roles in any organization to ensure diverse perspectives. The interviews in this case was open-ended questions. This technique was utilized to provide a rich and detailed data on personal perceptions and experiences. This allowed an exploration of what one can refer to as a nuanced insight which cannot be captured via surveys.

The second technique utilized in this case was on the focus groups. In here a focus group was conducted with diverse set of employees to discuss their experiences. This technique facilitated an interactive discussions and one which assisted to identify common attitudes and themes among the employees. Third technique employed in this case was the direct observations. In here the researcher observed workers or employees’ behavior in a simulated security scenario before and after security awareness training. The result was the development of an observation checklist which systematically recorded observed behaviors

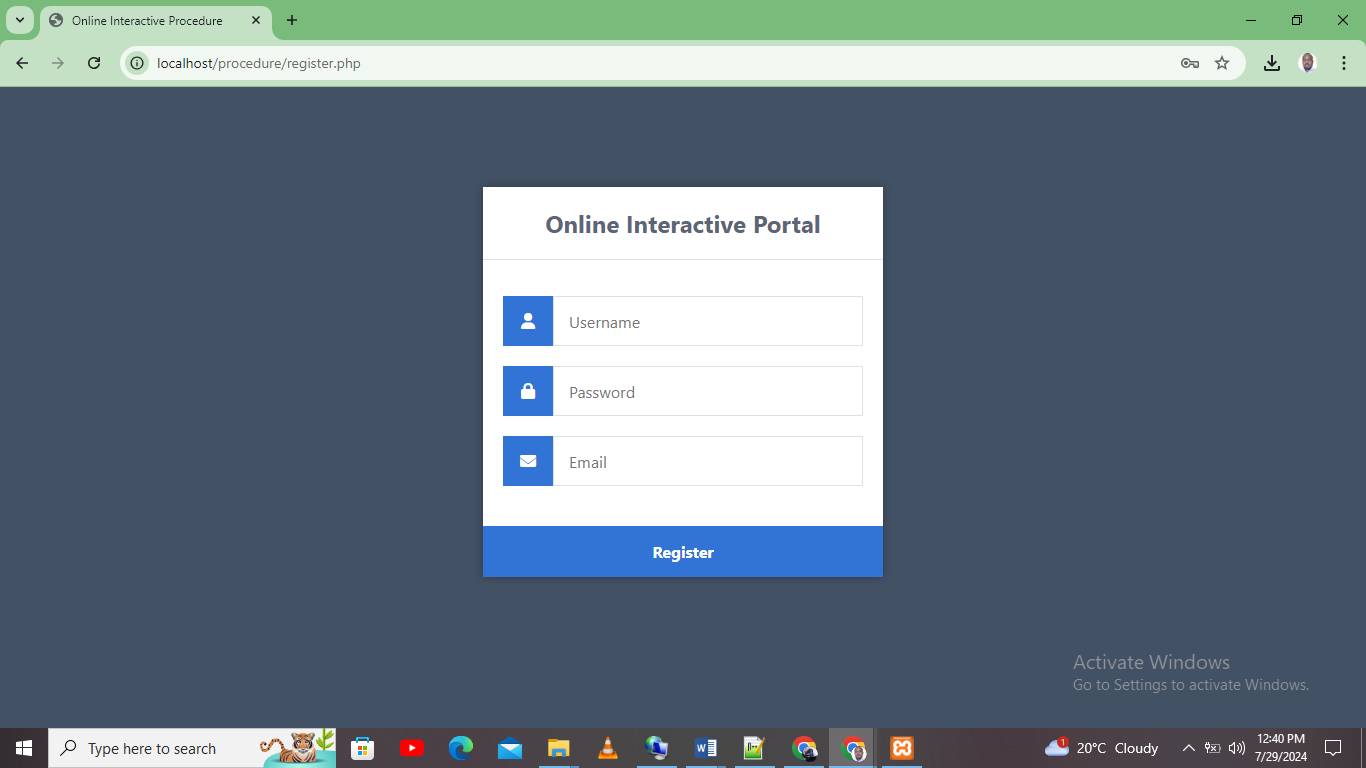
## **3.3 Online interactive procedure**

An online interactive procedure would be developed which addressing the key themes. This will be an online and interactive training modules which will be based in the findings from both qualitative and quantitative. Some of the interactive features like simulations, quizzes, and case studies would be incorporate to engage workers and to enhance the retention of knowledge.

Sample feature 1: Registration for users



Sample 2: The Login page for users



The online portal for assessing the effectiveness of security awareness programs requires a user friendly, scalable, and robust platform. The languages utilized in this case included PHP and HTML. PHP in this case was utilized as a server side scripting language. The language can generate a dynamic page which made it ideal for an interactive portal. Also it enabled an integration with the various databases such as MYSQL and PostgreSQL. The HTML language is a standard mark-up language for creating web applications and pages

## **3.4 Justification of mixed research methodology**

A mixed methodology in this case allows a comprehensive evaluation and exploration of the effectiveness of security awareness training. The combination of these mixed research approach ensured a thorough examination of the security training impacts from the various perspectives. Second is on the triangulation aspect; by using various data methods and sources it increases both validity and reliability of the findings. Lastly the qualitative aspect offers a deep and contextual insights while the quantitative technique offers a broad and generalizable data.

The development of an online procedure based on the research findings ensures that the study has what one can refer to as a practical implication for companies and organizations thereby offering tangible outcome which can be implemented to improve cybersecurity awareness among workers.

## **3.3 Research procedures**

To collect data a pre-training assessment is employed. The method in this case is to use an online survey and what one can refer to as knowledge assessment. The data collected in this case are multiple choices, self-assessment, and scenario-based questions. The aim here is to establish a baseline data on workers. Second is training program participation; in this case are the engagement levels. The aim here is to monitor workers’ participation

# **Planning and scheduling**

4.1 Gantt chart

|  |  |
| --- | --- |
| Item | Timeline |
| Proposal design and approval | 3 weeks |
| Research preparation | 1 week |
| Literature review on currently adopted training programs | 2 weeks |
| Data collection and analysis | 3 weeks |
| Findings preparation | 1 week |
| Report writing and preparation | 2 weeks |
| Online platform design | 1 week |

# **Progress to date**

|  |  |  |
| --- | --- | --- |
| Item | Timeline | Status |
| Proposal design and approval | 3 weeks | Done |
| Research preparation | 1 week | Done |
| Literature review on currently adopted training programs | 2 weeks | Done |
| Data collection and analysis | 5 weeks | Started |
| Findings preparation | 1 week |  |
| Report writing and preparation | 2 weeks |  |
| Online platform | 1 week |  |

# **Chapter 4**

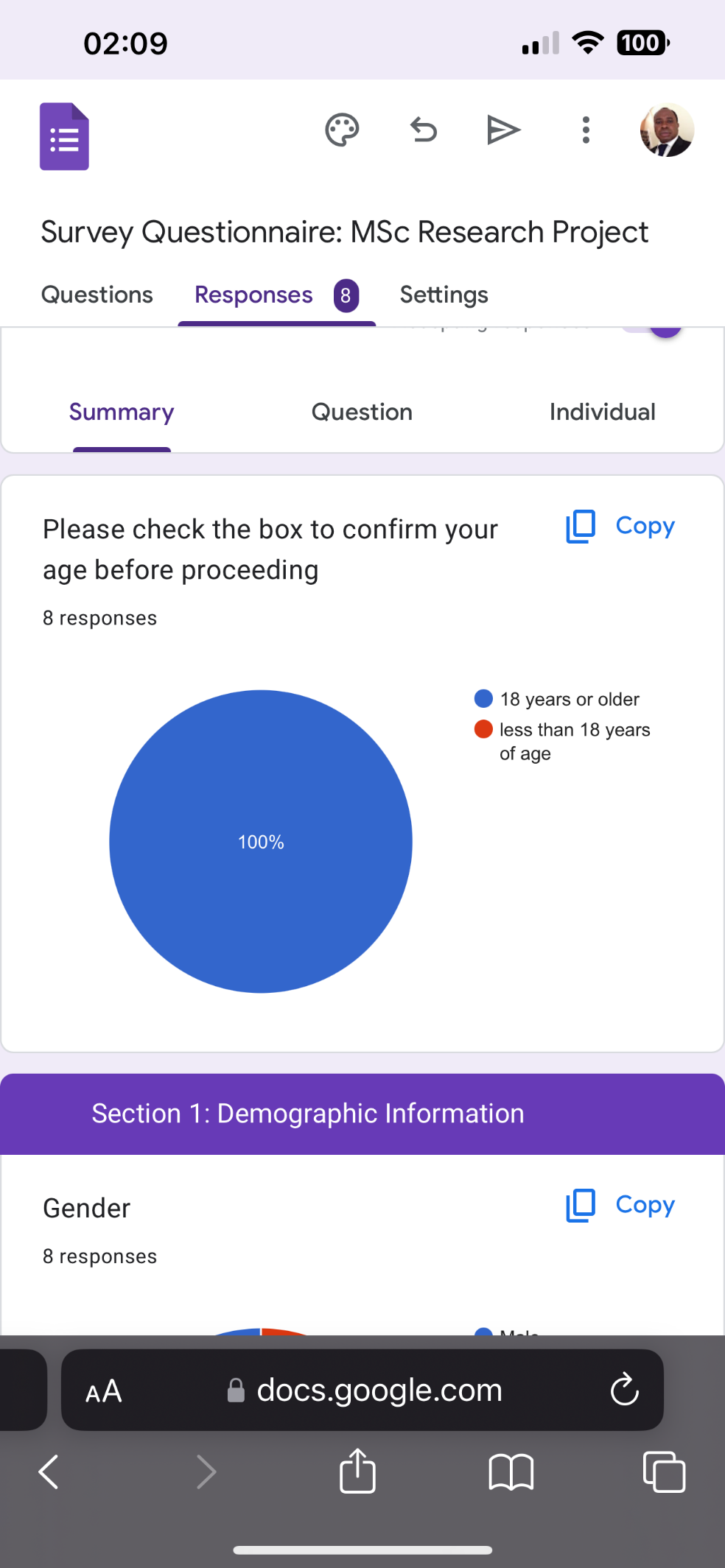
The data for this project was conducted using an online Google Form questionnaire. The participants submitted their responses and the data was captured. This section details a detailed visual presentation of the data collected.

4.1 Data presentation

4.1.2 Demographic analysis

First is that all the eight respondents were eighteen years and above. This is as shown by the figure 3 shown below. From the eight responses, 75 percent were male while the rest 25 percent were females. Additionally, 50 percent of the respondents were female and 37.5 percent were masters’ holders.

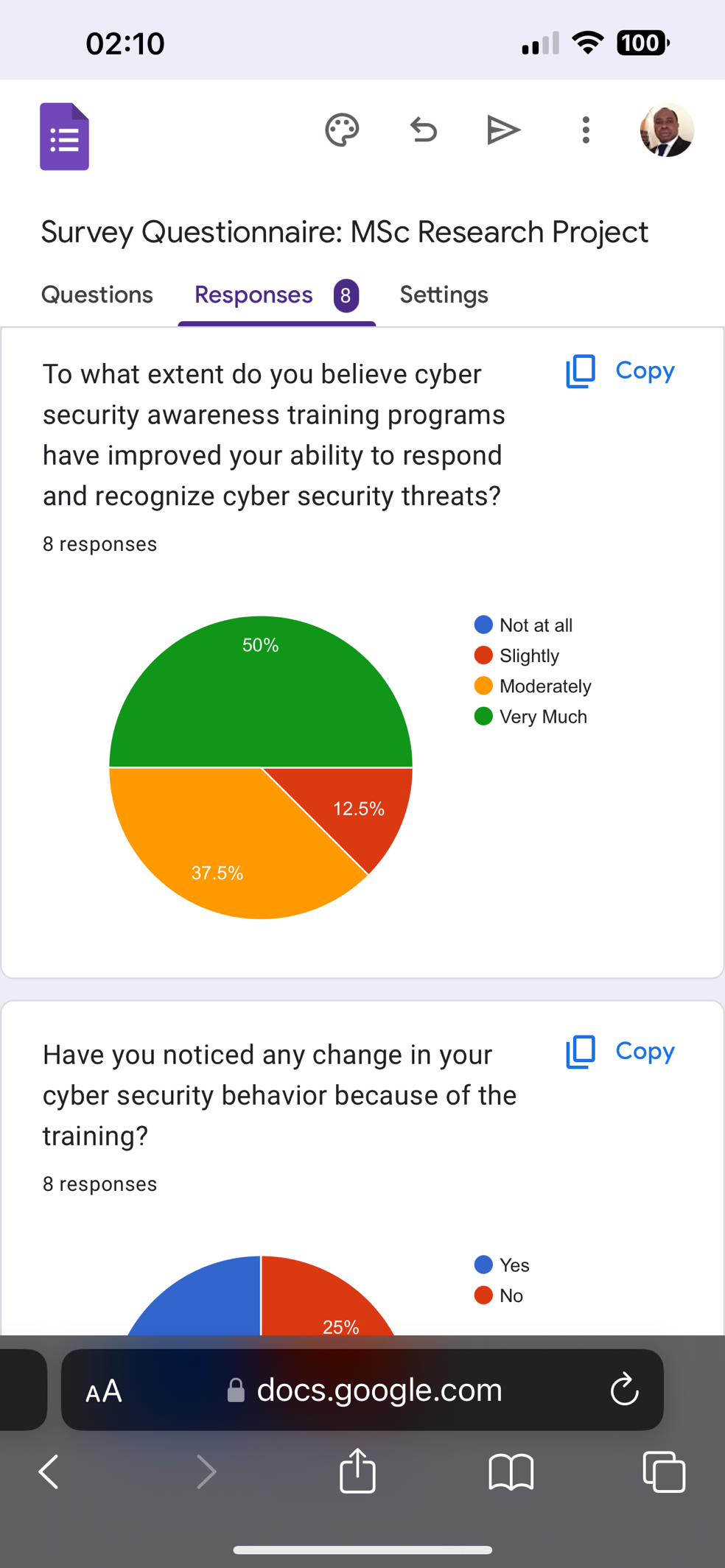
Figure 3: Age of the respondents from data collected

****

Second, the largest group of the respondents were the general staff and 12.5 percent from the IT department. This suggests that most of the respondents did not have an idea of what they might be exposed to when it comes to cybersecurity concerns

4.2 Pre-training security assessment

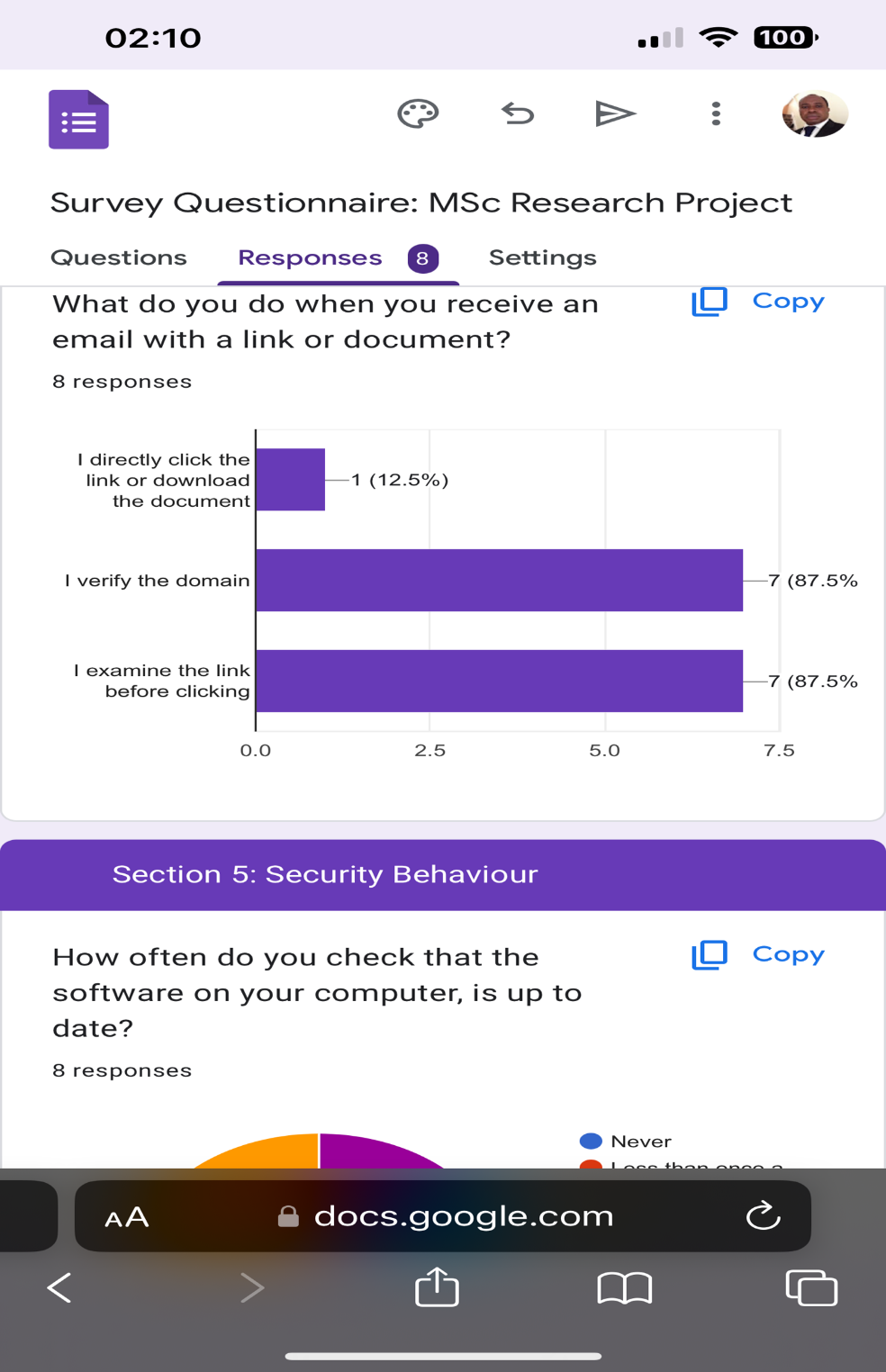
Fifty percent of the respondents indicated that they were familiar with the cybersecurity concept. This shows that half of employees had at least some before knowledge on cybersecurity. This one can indicate as a positive starting point. The rating on common cybersecurity threats skewed towards lack of knowhow on the cyber-security program awareness. Most of the respondents did not agree that cybersecurity program in their organizations improved the ability to recognize cybersecurity threats. In this case 50 percent of the respondents disagreed that cyber security training programs improved their ability to recognize and respond to cybersecurity threats this is as indicated by the graph shown below



4.3 Employee behavior

Email verification

From the data collected, the frequency of verifying the sender’s email was high. In this case all the respondents responded that they have the ability of recognizing phishing email attempts. This suggests a decreased vulnerability in most organizations as phishing attacks are eliminated. However, further training is needed as 12.5 percent of the respondents indicated that when they received an email with al link they never do any verification, they just download the contents of the email. This is as shown by the graph shown below



Additionally, password update among the employees remains a concern. In this case the data collected suggests that while two respondents update their passwords more often, three respondents do so sometimes, and the remaining three respondents never update their passwords. This showcases the need for a targeted intervention to improve the management of passwords

4.4 Post training security assessment

After the training they was a noticeable improvement from the data collected. From the eight respondents five of them responded that their rating was either Good or excellent. This showcases an effective training is paramount to enhance cybersecurity training awareness. Additionally, 6 out of the eight responses that this project received showcases that they were an improvement in able to verify a domain before opening an email. Nevertheless, two of three respondents did not report any improvement from the training. This indicates that training did not fully resonate with the participants thereby suggesting they be in place a better and interactive cyber security training awareness program

In general, from the data collected, the analysis from the survey data collected suggests a positive outcome from the cyber-security training awareness program. Additionally, key areas like email security and password hygiene still require further attention. The survey showcases that a continuous training is needed for a more enhanced process. Also the survey indicates that a more interactive is needed as some feel that the current cyber-security training never impacted their cyber-security awareness.

# References

EC-COUNCIL. (2022). *Certified Ethical Hacker Online Training | CEH Training - EC-Council Learning*. Https://Iclass.eccouncil.org/. https://iclass.eccouncil.org/our-courses/certified-ethical-hacker-ceh/#:~:text=Certified%20Ethical%20Hacker%20%7C%20CEH%20Certification&text=By%20providing%20an%20understanding%20of

ESET. (2021). *magazine*. https://web-assets.esetstatic.com/wls/2015/05/magazine.pdf

Hamdi, R. (2022). Cybersecurity Awareness in Saudi Arabia: A Systematic Literature Review. *Edulearn Proceedings*, *1*(2). https://doi.org/10.21125/edulearn.2022.1142

He, W., & Zhang, Z. (Justin). (2019). Enterprise cybersecurity training and awareness programs: Recommendations for success. *Journal of Organizational Computing and Electronic Commerce*, *29*(4), 249–257. https://doi.org/10.1080/10919392.2019.1611528

Hijji, M., & Alam, G. (2022). Cybersecurity Awareness and Training (CAT) Framework for Remote Working Employees. *Sensors*, *22*(22), 8663. https://doi.org/10.3390/s22228663

IBM. (2019). *IBM Study Shows Data Breach Costs on the Rise; Financial Impact Felt for Years - Jul 23, 2019*. IBM News Room. https://newsroom.ibm.com/2019-07-23-IBM-Study-Shows-Data-Breach-Costs-on-the-Rise-Financial-Impact-Felt-for-Years

IBM. (2023). *Cost of a data breach 2023*. IBM; IBM. https://www.ibm.com/reports/data-breach

Irwin, L. (2022, July 1). *Human Error is Responsible for 82% of Data Breaches*. GRC ELearning. https://www.grcelearning.com/blog/human-error-is-responsible-for-85-of-data-breaches

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees’ cybersecurity behavior. *International Journal of Information Management*, *45*(45), 13–24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017

Maersk. (n.d.). *STCW ISPS Security Awareness e-learning*. Maersk Training | Denmark Esbjerg. Retrieved March 16, 2024, from https://www.maersktraining.com/esb/course/stcw-isps-security-awareness-e-learning/

Sans Institute. (2021). *Cyber security training and awareness*. Sans.org. <https://www.sans.org/security-awareness-training/>

SANS . (2021). *Knowledge Assessment | SANS Security Awareness*. Https://Www.sans.org/Security-Awareness-Training/Products/Cyber-Risk-Insight-Suite/Knowledge/. https://www.sans.org/security-awareness-training/products/cyber-risk-insight-suite/knowledge/

Terrell, S. R. (2019). Mixed-Methods Research Methodologies. *Qualitative Report*, *17*(1), 254–280. https://eric.ed.gov/?id=EJ973044

University of California. (n.d.). *UC Cyber Security Awareness Fundamentals | People & Culture*. Hr.berkeley.edu. Retrieved March 16, 2024, from https://hr.berkeley.edu/grow/grow-your-skills/useful-learning-links/foundational-skills-required-training/uc-cyber-security#:~:text=This%20interactive%20Cyber%20Security%20Awareness

Verizon. (2023). *2023 Data Breach Investigations Report*. Verizon Business. https://www.verizon.com/business/resources/reports/dbir/

Xerox. (2019). *Cyber Security at Xerox*. Www.xerox.com. https://www.xerox.com/en-us/about/cyber-security

# **Appendix**

## **Sample Questionnaire**

Section 1: Demographic Information

1. Age









1. Gender





1. Department

IT

Finance

Procurement

Sales

Operations

1. Job Roles (Please list at least three of your job roles)
2. Years of Experience







**Section 2: Pre-training Security assessment**

1. Are you familiar with the concept of cyber-security?





1. Your rating on common cyber-security threats?







1. Have you received any formal training on cyber-security before?





If Yes, please specify the type of training which you have gone through

----------------------------------------------------------

1. How essential is cybersecurity in your organization?





**Employee behavior**

1. How often do you update your passwords? (Please tick where appropriate)

|  |  |
| --- | --- |
| Never |  |
| Rarely |  |
| Sometimes |  |
| Often |  |

1. How often do you verify senders email passwords before opening any attachments? (Please tick where appropriate)

|  |  |
| --- | --- |
| Never |  |
| Rarely |  |
| Sometimes |  |
| Often |  |

**Section 3: Post training security questions**

1. How would rate your knowledge of common cyber-security threats like phishing, malware infections after training

(Please tick where appropriate)

|  |  |
| --- | --- |
| Poor |  |
| Fair |  |
| Excellent |  |
| Good |  |

1. Has your ability to recognize phishing attempts improved after training?





1. How do you feel after training? Has the training improved your overall cyber-security awareness?





1. How likely are you to report and suspicious activities in the IT department of your organization? (Please tick where appropriate)

|  |  |
| --- | --- |
| Always |  |
| Rarely |  |
| Sometimes |  |
| Often |  |