AN INVESTIGATION AND EVALUATION INTO THE EFFECTIVENESS OF

SECURITY AWARENESS TRAINING PROGRAMME IN ORGANISATIONS

A Master’s thesis

Submitted to the Faculty

of

[University]

by

[Student’s Name]

In Partial Fulfilment of the Requirements for the Degree of

Masters of Science in Computing

December 2024

Capstone Professor: [Unit Professor’s Name]

This thesis titled “An investigation and evaluation into the effectiveness of

security awareness training programme in organisations” grants rights to the [university] for educational purposes only.

© Copyright 2024 by [Student’s Name]

All rights reserved.

# ABSTRACT

Security awareness is an important part of information security, mandatory for organizations that deal with regulated data, such as personal data, financial and health industries. One such awareness recommendation comes from ISO 27002 regulation and SANS Institute.

This study reviews previous research on security awareness training, evaluates the exiting literature regarding cyber security risks to pinpoint research gaps and proposes future directions for this area of study. The paper utilized survey methods and techniques to collect primary data. This enables the measurement of any changes in cybersecurity knowledge, self-reported behaviors, and attitudes.

The objective is to analyze how security awareness training programs impact employees' behaviors, attitudes, and understanding of cybersecurity. Additionally, it identifies measurable metrics for evaluating the effectiveness of these training programs, such as enhanced response times, increased reporting of suspicious activities, and a decrease in security incidents. Finally, the aim is to offer practical recommendations and insights for improving security awareness training programs based on empirical evidence. The goal is to find ways to enhance employee involvement in awareness training by suggesting an online, interactive platform where all employees can refresh their knowledge and skills related to security awareness topics and practices. The research employs both qualitative and quantitive methodology

The findings of the project were that cyber-security awareness is paramount. Also, the research observed that employee training on cyber-security addresses some of the key cyber-security threats. However, having an online interactive training portal is paramount as it acts as a means of post security assessment of the program utilized to training employees

TABLE OF CONTENTS

[COPYRIGHT 1](#_Toc185718053)

[ABSTRACT 2](#_Toc185718054)

[I. Introduction 5](#_Toc185718055)

[Chapter overview 5](#_Toc185718056)

[Background to the problem 6](#_Toc185718057)

[Justification for the research 8](#_Toc185718058)

[Research definition 9](#_Toc185718059)

[Objectives 11](#_Toc185718060)

[II. LITERATURE REVIEW 15](#_Toc185718061)

[Overview 15](#_Toc185718062)

[Current existing cyber security training programs adopted by organizations. 15](#_Toc185718063)

[Case studies 19](#_Toc185718064)

[Case study 1: SANS institute 19](#_Toc185718065)

[Case study 2: Xerox Corporation 22](#_Toc185718066)

[Case study 3: University of California, Berkeley 23](#_Toc185718067)

[Best Practices and Strategies 26](#_Toc185718068)

[III. METHODOLOGY 27](#_Toc185718069)

[Methods and techniques selected. 27](#_Toc185718070)

[Data collection methods 28](#_Toc185718071)

[Qualitative research methods 29](#_Toc185718072)

[Qualitative data collection methods 30](#_Toc185718073)

[Online interactive procedure 30](#_Toc185718074)

[Methodology Justification 32](#_Toc185718075)

[Research procedures 32](#_Toc185718076)

[IV. DATA PRESENTATION AND ANALYSIS 36](#_Toc185718077)

[Overview of the Problem 36](#_Toc185718078)

[Data analysis and findings 36](#_Toc185718079)

[Data and modelling approach 37](#_Toc185718080)

[Results of Data analysis 37](#_Toc185718081)

[IV. ONLINE INTERACTIVE TRAINING PORTAL DEVELOPMENT 44](#_Toc185718082)

[Overview 44](#_Toc185718083)

[System requirements 45](#_Toc185718084)

[Functional requirements 45](#_Toc185718085)

[Non-functional requirements 50](#_Toc185718086)

[Architecture design 51](#_Toc185718087)

[4.3.1 Front-end architecture 51](#_Toc185718088)

[Back-end architecture 51](#_Toc185718089)

[Purpose of the Online training portal 52](#_Toc185718090)

[Interpretation of the results 54](#_Toc185718091)

[Connecting to the literature review 54](#_Toc185718092)

[VI. CONCLUSION. 55](#_Toc185718093)

[References 57](#_Toc185718094)

[Appendices 63](#_Toc185718095)

[Appendix 1: Planning and scheduling 63](#_Toc185718096)

[Figure 6a: Schedule and research plan. 63](#_Toc185718097)

[Appendix 2: Gantt Chart Planning and Scheduling table 64](#_Toc185718098)

[Appendix 3: Progress to date. 67](#_Toc185718099)

[Appendix 4: More on Online iterative portal. 70](#_Toc185718100)

[Database 70](#_Toc185718101)

[Figure 1:1 Online iterative: phpMyAdmin 70](#_Toc185718103)

[Figure 2:4 Additional informational secti 76](#_Toc185718105)

[Appendix 5: Survey questionnaire 76](#_Toc185718106)

[Sample Questionnaire 77](#_Toc185718107)

An Investigation and Evaluation into The Effectiveness Of

Security Awareness Training Programme in Organisations

1. **Introduction**

## **Chapter overview**

In the past decade, the essence of security awareness training in cybersecurity risks mitigation has been widely recognized across various industries. Nevertheless, the effectiveness of such training in organizational cyber security posture remains a subject of debate. Awareness initiatives are designed to tackle specific weaknesses within an organization, resulting in outcomes that are unique and often evolving. It is challenging to make broad assessments about the overall effectiveness of security awareness programs, given their diverse nature. Nonetheless, it is beneficial to explore success stories and case studies to identify effective practices in awareness training. While no empirical data has been gathered, there are various success stories showcasing different methods, from traditional educational techniques to innovative, cutting-edge strategies. This section explores the current existing articles, case studies, and scenarios to evaluate the impact of security awareness training.

## **Background to the problem**

In the current digital age, cyber-security threats have proliferated and presented a significant challenge to organizations across all the sectors. These challenges include human error, accidental misuse, untrained employee, system failure, insecure network, and noncompliance attitude of staff (Palanisamy et al 2020). According to Parthy and Rajendran (2019), noncompliance behaviour of employees could violate the security of information requirements. Cyberattacks include the use of malware, phishing, trojan, social engineering and other forms of security attacks (Mathews S 2020).

Cyberattacks ranging from insider threats, phishing frauds pose security risks to the organization integrity, confidentiality, and available of sensitive data and the critical systems. As companies increasingly rely on digital technologies to store vast amounts of data and conduct their daily operations, the impact of cyber incidents on organizations operations, reputation, and financial stability are call for concern.

Amidst the cyber evolving threats and landscape, workers represent both a critical line of while technological solutions like intrusion detection systems, anti-virus, and firewalls used continuously and play a vital role, human negligence and error remains one of the significant contributors to security breaches. According to IBM report of 2023, the cost of human error can result in huge cost. Some cost is related to fraud cost which can cost organizations to about $5 per record stolen. As a result, about fifty-one percent of organizations worldwide are planning to invest in security awareness and to include tests, employee training, and threat detection (IBM, 2021).

From the two major reports it is evident that a substantial proportion of cyber security incidents attributed to human factors which includes falling victims to phishing attacks, clicking of malicious links, and mishandling of sensitive information. As earlier stated, few organizations have implemented security awareness training programs. Effective security awareness training is highly recommended by many security standards such as those mandated by HIPAA, IBM, and Calder (Rodrigues et al. 2024). These training programs is aim at educating workers about the current common threats and promoting the best cyber security practices. These initiatives usually include online modules, simulated phishing exercise, interactive workshops, and informational campaign designed to equip employees with skills and knowledge to mitigate and recognize potential security risks.

Despite these widespread recommendations of security awareness training programs to cybersecurity threats, questions remain on the effectiveness of awareness programmesin 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 behaviour 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 organisational security posture presents a methodological issue.

Against this gap and backdrop, there is a need to have comprehensive research to evaluate the efficacy or the effectiveness 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 defence of IT assets to reduce the likelihood of the current costly security breach.

**Justification for the research**

In the current existing research on security awareness 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 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 programs. This is so because there is a 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 improving the various training initiatives.

This section explores the exiting knowledge and literature related to security awareness training, including its definitions. It also highlights the need for organizations to invest in security awareness training programs to mitigate the increased risks and threat associated with cybersecurity breaches. It identifies the gaps in current research and identifies the significance of conducting this study given the limited existing literature on the measurable differences resulting from security awareness training initiatives.

## **Research definition**

**The practical problem** in this case the practical issue is security awareness training program used to mitigate cybersecurity threats. The practical issue revolves around determining whether the training programs make a tangible difference in enhancing workers security behaviours 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, translating the gained knowledge from training into a secure and consistent behaviour. 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. According to Alkhalil Z et al, (2021) and Gupta et al, (2015) Social-engineering-based attacks is the favorite approach for cyber criminals to attack users and get them to click on link to get access to their information’s. Human vulnerabilities are exploited using various psychological tricks to manipulate and exploit human minds in other to gain access to their information is concerning. (Parthy and Rajendran 2019), recommend regular security awareness training for all employees.

Depriving employees of security awareness training could lead them to exposing an organization’s confidential information unwittingly. (Palanisamy et al. 2020). Some researchers conclude that training plays a vital role in shaping the behavior of employees regarding information sharing, creating positive change in employee behavior and increased risk awareness. What is not clear is how effective is employee engagement in identifying risk in the long term.

Social engineering involves manipulating individuals to show confidential information for illicit purposes, which may include sensitive data like login credentials. Participants in the phishing simulation, guided to react to the simulated phishing emails. Phishing simulators offer computer-based training exercises that replicate genuine phishing situations within a safe environment. According to Younis and Musbah (2020), it is vital for the crafted phishing emails to appear highly realistic to keep trust with employees. The simulation yields two key insights about human behavior: it tracks the number of employees who clicked on the phishing emails as well as those who went a step further by entering their sensitive information, such as usernames and passwords, on a fake phishing site. Additionally, phishing simulators can produce conventional metrics like click-through rates (Jampen et al., 2020)

GestureWare, Inc., on request, uses interesting and educational methods to train employees. They find that because the process is not forced or mandated, employees respect the approach and go out of their way to remember examples of the solicited items. (Ciudin et al.2024)

Costco Wholesale employs a computer-based training and assessment system that actively engages learners and evaluates their understanding. The training material combines static content with interactive elements. Each day, the information security officer receives an email report detailing employee participation. Additional effective measures include a clear policy statement and posters that remind staff of their security responsibilities. (Salisbury, 2024).  **Research Objectives**

The aim of this paper is to analyses the effectiveness of security awareness training and provide valuable insights for organizations seeking to enhance their security posture. By examining various aspects of security awareness training programs, this section aims to identify key factors that contribute to successful outcomes.

This study aims to assess the effectiveness of security awareness training programs in proving employees’ knowledge, behaviours, and attitudes towards cybersecurity. It also seeks to contribute to the existing body of knowledge by investigatingthe extent to which various awareness training programs influences measurable outcomes such as reduced security incidents, increased adherence to policies, and improved incident response capabilities.

**Objectives**

The objective is to provide conclusive data that will enable organizations to make accurate decisions relating to their security awareness training initiatives. The research will revolve around four major objectives.

1. To examine and determine the extent to which security awareness training programs influence workers’ behaviours, 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 suspicious activities, and reduction in security incidents.
3. To provide actionable recommendations and insights for optimizing security awareness training programs based on empirical findings.
4. To identify means of improving employee engagement in awareness training by recommending an online / interactive site to help all employees to refresh their knowledge and practice on security awareness training issues and practice.

Information on method, task, and deliverable are in the table below.

**Objective 1:**

|  |  |  |
| --- | --- | --- |
| **Method** | **Task** | **Deliverable** |
| literature search | Using OU library or google scholar to obtained literature on awareness training. | Read books and journal that articles outline cybersecurity risk and best practice. Collect secondary data for analysis to determine any gab. |
| Mixed method of research | Using a prepared questionnaire and survey conducted to understand effectiveness of the knowledge gained | Data gathering, data analysed and interpretation. Collect data to determine workers behaviour. |
|  | Implement design | Tests perform |

**Objective two.**

|  |  |  |
| --- | --- | --- |
| **Method** | **Task** | **Deliverable** |
| Literature search | Using web search and UO library to  obtain relevant paper, take note, and analyse | A write-up of literature survey, gather data, analyse to determine the level of training effectiveness |
| Qualitative and quantitative  method | Conducting surveys or gathering of  feedback through questionnaire,  (employee feedback), pre-training assessment, participation rate, phishing simulation results, Quiz scores security incident metrics, compliance metrics | Questionnaire developed, perform test, and write TMA04. To present the level of current effectiveness. |

**Objective three**

|  |  |  |
| --- | --- | --- |
| **Method** | **Task** | **Deliverable** |
| Mix method | Read and analyse both secondary and primary result. Implement design | Obtain and analyse data. Addressing the gab with recommendation. |
| Data analysis | Combine the result from objective 1 - 3 through quantitative analysis to form recommendation | Conclusions reached. Suggest two option of employee training portal that is cost effective and user friendly. |

**Objective four**

|  |  |  |
| --- | --- | --- |
| **Method** | **Task** | **Deliverable** |
| Research on online/  interactive site | Using website to collect information and design online interactive portal. | Tests perform, conclusion reached. Present online interactive portal, and write TMA04 |

The process of this research is first, the secondary research, which includes literature searches, reading, and data gathering. The second process is the primary research. this includes research design, planning, execution, talking to experts in the field, recording data, and data analysis. A survey questionnaire contains both open and closed question, sent out to recipients through online and collected after few weeks for analysis. The target is to get 50 respondence for the analysis. See section five of data analysis technique. Lastly, drafting my dissertation. Adopted from module material.

# **LITERATURE REVIEW**

## **Overview**

This chapter highlights in details the current existing reviews related to the study. Mainly the section highlights in detail the current existing cyber-security training programs adopted by organizations. Additionally, the section details real cases of training programs by organizations

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

A survey conducted in Hanover, Germany (12 January 2023), Hornet security (2023), found that 33% of company are not providing any cybersecurity awareness training to employees who work remotely. The research also found that 74% of employees working remotely can access important data, leading to increased security risks for companies in the evolving hybrid work environment. The study identified two key issues leading to risk: the accessibility of sensitive data by employees, and a lack of sufficient training on cybersecurity management and prevention of cyber-attacks or breaches. The screenshot below are statistics from Hornet security cyber security report.

A blue pie chart with a fish skeleton and a virus

Description automatically generated

Figure 2.2. Screenshot from Hornet security (2023): Attack type usage’

The data above shows that there is an increase in human error in 2021 and 2022 with phishing having the highest rate of 24.8% to 39.6%. This may be due to inadequate of awareness training, noncompliance to security policy and feedback.

According to cyber security magazine, cybersecurity global crimes will rise by 15% 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 defence 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 programs by organizations is the Certified Information Systems Security Professionals. This is a certification 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 include the principles of security, in this case the CIA principles. Second is 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 cybersecurity models, cyber security design frameworks and principles. Examples 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 training program to ensure their teams have a solid foundation in security practices and principles.

Certified Ethical Hacker is another security program widely adopted by most organizations. The EC-Council offers the program. The awareness focusses on practicing and understanding the hacking techniques to identify weaknesses that exist in one system. Also, 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 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 attacks such as, exploiting IOT devices and taking advantage of AI to launch sophisticated attacks is not cover in this program.

Other various study related to the topic conducted is that by Darem and others. The study addresses the growing threat of spear phishing, one of the common phishing attacks designed to trick people within an organization. The study has focused on evaluating the effectiveness of training techniques in improving workers’ ability to recognize and respond to spear phishing attempts. The spear phishing cybersecurity threat poses a significant risk due to its personalized nature. According to the authors its success rate is high. The articles proposed having in place an embedded solution that integrates the training elements directly into regular work activities to provide important and timely learning chances. The article aims to compare the impacts of embedded training with the traditional methods.

The authors employed quasi-experiment which involved two groups within a large organization. The data collected in this case included a pre and post training survey which measured the changes in workers’ attitudes and behaviors towards phishing. Also, data collected via a simulated phishing test; this was to assess the ability of workers to recognize and respond to spear phishing attempts before and after the training. The authors analyzed a click through rate on phishing mails, response times, and the accuracy of identifying phishing attempts to determine the effectiveness of training techniques. The major findings by the authors are that embedded training groups demonstrate an improvement by workers to recognize spear phishing mails as compared to controlled groups. Immediately. feedback provided by embedded training assists to reinforce learning and at the same time improve the detection rate.

Another finding by the article is that training groups exhibit more cautious behavior and a better adherence to the security protocols. Also, according to the article is that this technique is likely to report suspicious emails. Lastly, the authors listed the advantages which are associated with embedded training which includes contextual relevance, providing immediate feedback, and a higher engagement with workers is more likely (Darem, 2021).

While the study focuses on sustainability and behavior changes in the short term and immediate impacts on embedded training, it does not provide data on long term sustainability. Some research in this case is needed to evaluate whether improvements in phishing recognition among employees are maintained over an extended period. Second, while the study uses click-through rates and the response times as the major tactics, it lacks a comprehensive set of evaluation metrics that measures the overall effectiveness of embedded training.

## **Case studies**

### **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 corporations to develop a customized security awareness training program 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 Institutes, 2021).

One of the examples 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.

A survey conducted by SANS institutes in 2023, contains data from approximately 2,000 security awareness practitioners around the world (about eighty countries). SANS report of top human risks which includes phishing/vishing/smishing, passwords/authentication, detection/reporting, IT admin misconfiguration. Figure 2.2 below shows respondents cited one risk above the others. On the top risk identified is social engineering attacks (phishing and vishing attack) followed by password/strong authentication and detecting/reporting incidents. This imply that human error will always be a matter of concern if not well check and apply regulation.

**A blue bar graph with black text

Description automatically generated**

Figure 2.2.1 Screenshot: Lance S (2023). SANS 2023 Security Awareness Report: Managing Human Risk.

The literature review conducted indicates a strong view from researchers of ensuring employee awareness training. This will not make any measurable differences if there are no Continuous learning and Improvement, adequate method of feedback and incident respond training, simulated phishing exercises, promoting a security culture, simplify training program and accurate update of the current trend of cyber attach that will enable the development of new awareness program to mitigate the new trend of attack. Grimes noted that the key to addressing security challenges caused by human mistakes is through education. This includes learning about misconfiguration errors, the significance of patching, stolen credentials, or even common errors like sending data to the wrong recipient accidentally.

#### 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 organization’s culture evolved with workers actively participating in adopting shared responsibility and cybersecurity initiatives for protecting organizational assets.

However, while the SAN’s institute case study offers valuable insights into the effectiveness of security awareness training programs, there are areas or gaps that need pointed out. First, the case study does provide 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 immediate outcomes following the implementation of security awareness programs. For example, the case study only points out reduction of security incidents because of cyber security awareness programs. The case study does not delve into 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 mentions 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 program 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.

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

The second case study is the Xerox corporation, the company faced issues related to information security data breaches. As a result, the company decided to conduct security awareness training program for all its employees. The security awareness program was aim at educating employees about the various cybersecurity risks and promote the best practices for safeguarding company sensitive information. The security training module conducted by cybersecurity experts include interactive modules, in-person workshops, and conducting simulated phishing exercises.

After conducting the security awareness training program, Xerox reported a reduction in security incidents which where link to employee negligence like accidental data leaks. Second, is that employees demonstrated an improved awareness of social engineering tactics and phishing frauds. This led 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). The company has developed Xerox Cyber threat management portal to share information with audiences

The portal is known as Xerox CSCC portal more about the portal you can get (https://www.csoconference.com/wp-content/uploads/2018/01/CSO50\_Xerox\_DRuss.pdf)

The portal is located at (<https://www.accounts.xerox.com/auth/login.jsf?locale=en_US>). But data can be retrieved without having to sign in.

#### Gaps in the case study

Even though the 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, link to 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 a 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.

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

The third case study is the University of California case study. The institution reported continuous cybersecurity issues and data breaches affecting its students, staff, and faculty. As a result, the university decided to conduct a cyber-security awareness program targeting its students and staff. The training includes online modules, awareness campaigns 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. Incident response capabilities heightened, and students demonstrated improved cyber security best practices, (University of California, n.d.).

The university also conducted a campaign that bring people across campuses together to learn how to develop a systemwide security mindset, using AI automation and incident response testing to address cybersecurity concerns. Figure 2.2.3a show 97% satisfaction rate. While figure 2.2.3b show significant changes in between 2022 to 2023 (UC Cyber risk Program 2023). The Cyber-risk Coordination Centre (C3) has released its 2023 Cyber Risk Program Annual Report, which emphasizes the strategies, individuals, services, and tools utilized to manage and mitigate cyber risks across all UC campuses, health centres, and labs.

The report showcases various achievements and improvements made in cybersecurity within the UC system over the past year. Notable points include:

- UC Berkeley's initiative to share best practices for policy implementation

- UCLA Health's enhancements to phishing simulations that offer better learning experiences, including communication with executives during cyber incidents

- The popularity of privacy workshops at UC San Diego

- A $20 million grant for AI-driven cybersecurity efforts from UC Santa Barbara

- UC San Francisco’s early adoption of Attack Surface Management services. See figure 2.2.3b

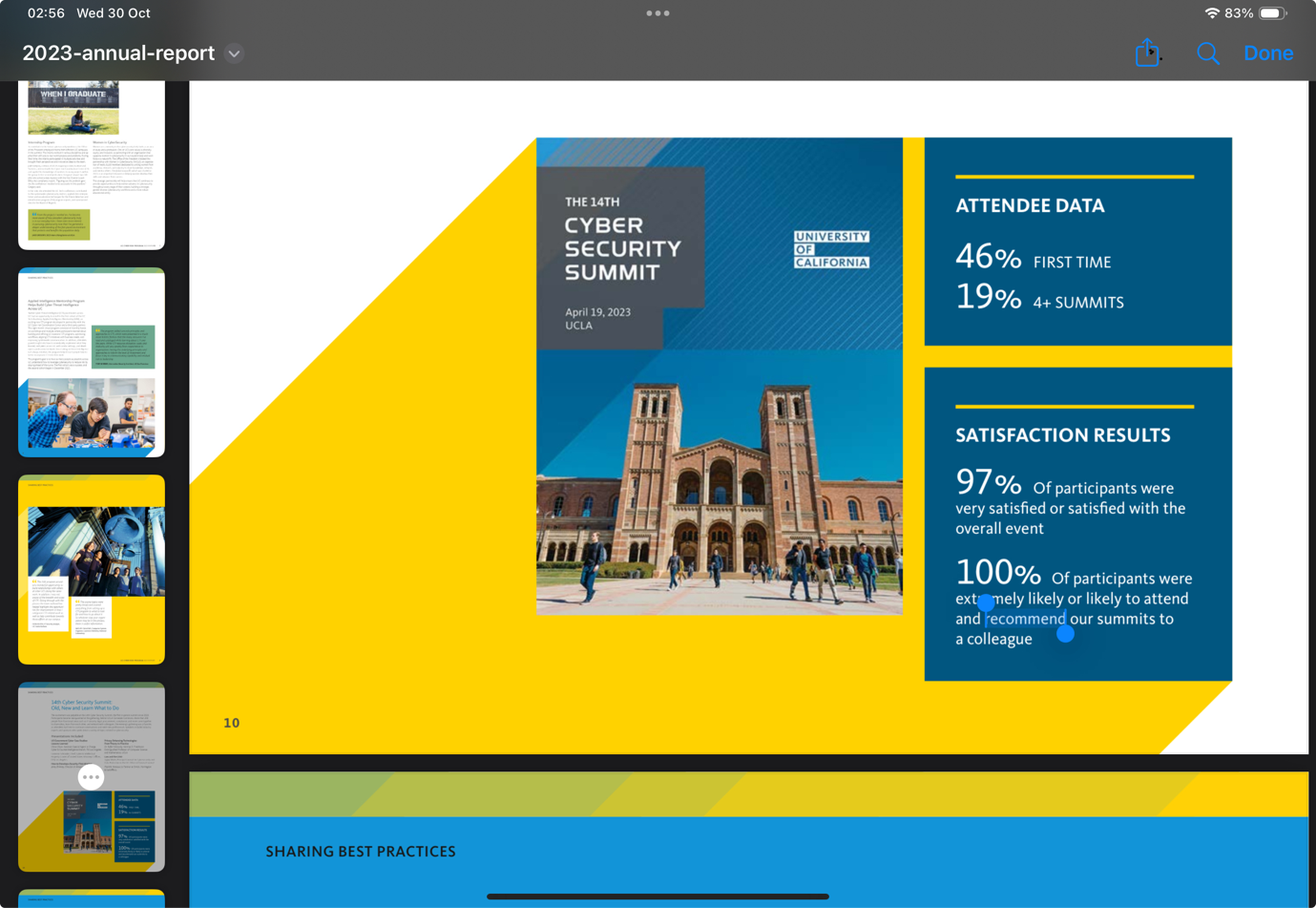


Figure 2.2.3a Screenshot of Satisfactory report of attendee (UC Cyber risk Program 2023)

****

Figure 2.2.3b A screenshot of the Landscape 2023 report (UC Cyber risk Program 2023)

#### Case study gaps

As highlighted above, the university cyber security awareness program tailored towards students and staffs which resulted in a decrease in authorized access to university systems and data. However, the case study lacks quantitative metrics which used to measure 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 does not delve into long term sustainability. Lastly, even though the case study mentions that the training initiative targets the staff and students, it does not detail 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.

## **Best Practices and Strategies**

The best practiced and strategies as conclusion, derived from case studies above: Critical Security Controls recommend that effective security awareness training ensures all employees understand security risks and can engage in activities that mitigate threats (Khando et al., 2021) (McIlwraith, 2021). To keep staff informed, the guide advocates for incorporating monthly updates in newsletters along with reminders about physical security. Additionally, it is crucial to conduct simulations and manage both internal and external digital social engineering attacks through penetration testing. These pen tests evaluate individuals’ ability to safeguard their environment, encompassing digital technology, policy compliance, encryption, and physical security considerations, including human factors.

Continuous reinforcement is another important aspect of security awareness training, according to HALT. It is important to follow up initial in-depth training with reminder notices and department briefings to ensure that employees understand and remember what is expected (Griffin, 2021).

Awareness training is vital for organizational security, as robust IT security relies not only on advanced technological solutions but also on the behaviours and attitudes of individuals. Effective security awareness training should ensure that every employee recognizes security risks and is engaged in reducing these threats. Despite many organizations implementing security training, few have clarity on the content, methods, and frequency of their programs. This chapter offers a detailed examination of suitable measures and recommendations for creating an effective security awareness training program.

# **Methodology**

## **Methods and techniques selected.**

The research design aligns with the constructivist paradigm, which involves examining "multiple social realities." A mixed-methods approach was employed, collecting qualitative data through individual interviews to investigate various aspects of Security Awareness programs, while quantitative data were gathered through surveys to assess employee responses to phishing and to estimate the return on investment for phishing testing. The qualitative component aims to understand the dynamics around security awareness initiatives, while the quantitative aspect focuses on measuring employee reactions to phishing attempts. Utilizing a mixed-methods strategy enhances the reliability of the results by "triangulating" the data, allowing for the verification or reduction of personal bias using multiple data sources. Specifically, by comparing qualitative and quantitative findings, researchers can cross-check emerging patterns for a "richer, more nuanced" understanding. A stratified sampling of staff was implemented to improve the generalizability of the results, categorizing staff based on factors like authorization levels, job roles, and age groups to establish a representative sample. In-depth interviews with selected representatives from each stratum meant that a large sample size wasn’t necessary.

Based on the gaps identified from the literature review, and the critiques provided, mixed approach research methodology is used in 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 the quantitative phase. In here a survey questionnaire developed based validated measures and scales identified in the literature review. In this case, these measures would be security self-efficacy, perceived barriers, and what I can refer to as response efficacy. Also, here the study utilizes what is known as stratified sampling technique used to ensure that there is a representation across various organizational sectors. Questionnaires are design to assess users’ cybersecurity awareness, behaviours, and attitude. See appendix 2 for designed survey questionnaire. Lastly, a statistical analysis like Structural Equation Modelling (SEM) and regression analysis needed to examine the relationship between the various variables (Terrell, 2019).

In this research, both qualitative and quantitative data hold equal significance for several reasons. The primary aim is to compare the perspectives of individuals, specifically business managers, who engage in both security awareness training tasks. This study looks to encompass a broader range of participants from various environments affected by security awareness, ensuring a better alignment between the individuals involved and the themes being explored.

## **Data collection methods**

This subsection outlines the methods employed for data collection in this study, emphasizing their importance to the research process. The methods examined include surveys, interviews (including in-depth interviews), direct observations, and a combination of interviews and observations. While data collection methods are not inherently biased, their discussion is crucial due to the study's focus on security awareness training within a business context. The primary aim is to understand the nature and effects of such training on the susceptibility of higher education staff to spear-phishing attacks.

In line with the research goals, an online survey was chosen as a suitable method. This approach facilitates the collection of a substantial number of responses and generates descriptive statistics. It allows for both quantitative and qualitative insights into the issue. The survey can encompass a wide range of individuals who have either experienced or are currently undergoing training. Additionally, in-depth interviews were incorporated into this mixed-method approach to provide richer insights and a more thorough analysis of the problem.

### **Qualitative research methods**

One of the techniques utilized to collect data is survey. The use of survey method in security training programs allows measure the changes in cybersecurity knowledge, self-reported behaviours, and attitudes. Survey distributed to participants one week before the training and after three months after the training to access the long-term impacts. The questionnaire sent through email to respondent and online for random participant. The questions in this case were Likert based on a scale of 1 to 5 and multiple-choice based questions. (See appendix 2)

The survey’s data collection method implemented as it provides efficient way to gather data from participants. Also, it provided quantifiable data used to statistically analyse or detect changes over a period. The pre and post training comparison can be to highlighting 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 done after and before the security awareness training program. The pre-training incident data, 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 used as it provided objective and real-world data on security incidents. Also, it provides a way to analyse incident trends before and after the training. This in turn revealed the training’s impacts on the actual security incidents practices.

### **Qualitative data collection methods**

One of the techniques 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 were open-ended questions. This technique 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 captured via surveys.

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

See link to the online survey <https://forms.gle/MCsQ9dmtxb9QtN8BA>. And Appendix 3: Survey questionnaire

## **Online interactive procedure**

An online interactive procedure developed which addressed the key themes. This is an online and interactive training module based on the findings from both qualitative and quantitative. The interactive features like simulations, quizzes, and case studies incorporated to engage workers and to enhance the retention of knowledge. See figure 3.1 and 3.2 of the online interactive. A second option that is less technical and can be used for quick training and awareness is also recommended. See Appendix 2

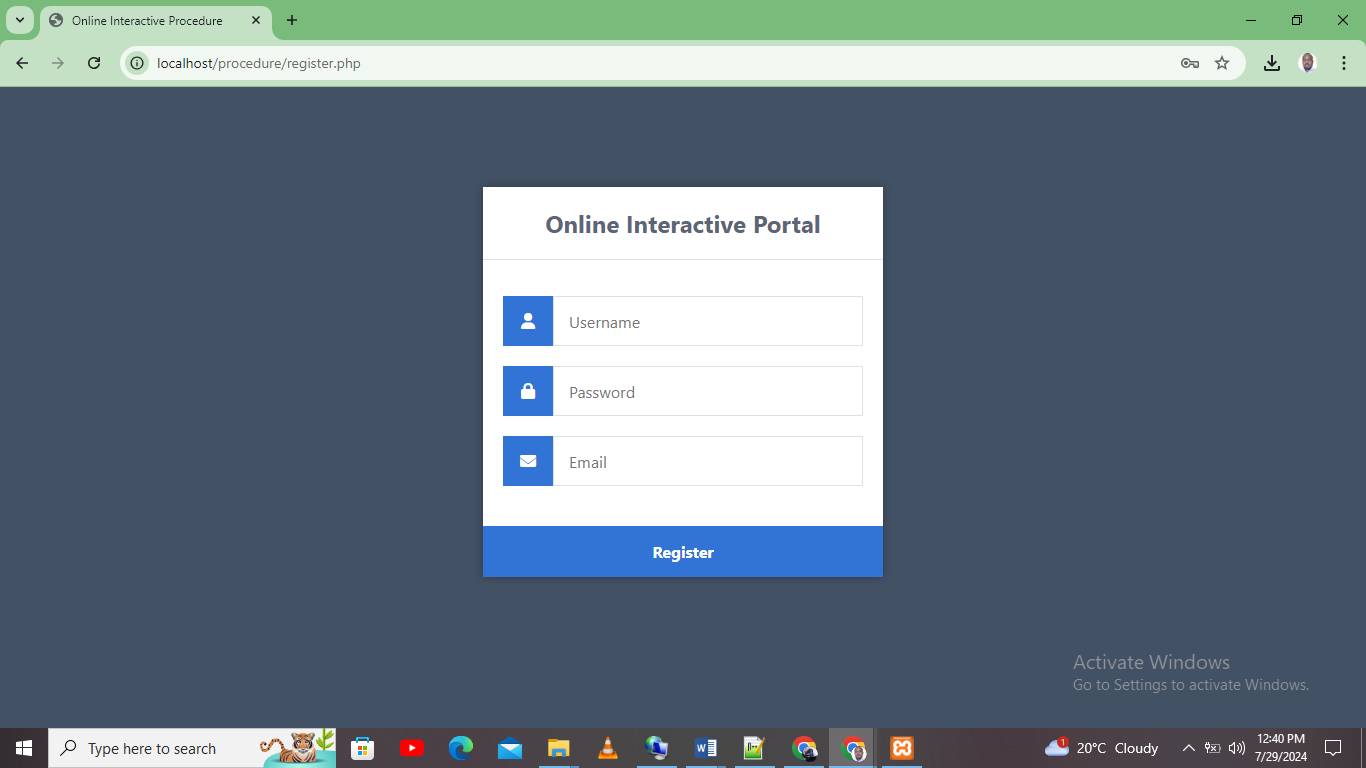


Figure 3.3a. Screenshot of the online designed portal

A screenshot of a computer

Description automatically generated

Figure 3.3b Screenshot of the online interactive Login portal

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. is utilize as a server-side scripting language. The language can generate a dynamic page which made it ideal for an interactive portal. Also, it enabled 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. Research shows that awareness training can make a significant difference if done regularly and frequently. This idea is not only cost effective but also engaging, reduces time and encourages users.

## **Methodology Justification**

A mixed methodology in this case allows a comprehensive evaluation and exploration of the effectiveness of security awareness training. Also, the methodology and triangulation of the findings from various sources will enhance the reliability and validity of the results. 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 implemented to improve cybersecurity awareness among workers.

## **Research procedures**

The methodology of this research includes secondary research where literature searches, reading, evaluation, and reviewed of data. Secondly, Primary research includes research design, planning, execution, talking to experts in the field, recording and analyzing data. Questionnaires Designed and sent out online and conduct interviews. Lastly, the writing stage of the research.This research employed an iterative lifecycle model which allowed feedback, review, and implementation of current ideas as the work progresses. The model includes planning, analysis and review, design, and implementation.

|  |
| --- |
| Planning |

|  |
| --- |
| Analysis |

|  |
| --- |
| Design |

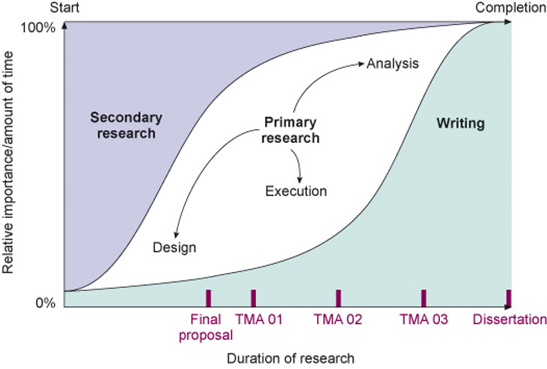
|  |
| --- |
| Testing |

|  |
| --- |
| Implementation |

Figure 3.1. Iterative lifecycle model.

This model allows changes to project as one received feedback from tutor. So far different amendments have taking place. This includes topic refinement, schedule plan, literature reviews and case studies and design of questionnaire.

The research is plan by formulating the research question based on the objectives. The planning ensures relevant literature and suitability of search strategy. Using reliable database, specific keywords and phrases were employed to extract data that are relevant to the research objectives. The planning, conducting, and review of literature occur in the secondary research. The primary research includes the design stage, execution, and data analysis. Finally, the writing stage. See figure 3.3 (Open university 2012)



A screenshot, figure 3.3 (Open university 2012)

Data collection in this study involves two main methods: surveys and observation. Surveys conducted to gather quantitative data on participants' knowledge, attitudes, and behaviours related to security. The surveys will include both closed-ended and Likert-scale questions, allowing for statistical analysis (Baburajan et al.2022). Additionally, observations conducted during training and after the training sessions to capture qualitative data regarding participants' engagement, interactions, and reactions to the training materials. (Husband, 2020). The target in this survey are any IT professionals, managers, and employees who are organizational assets owner.

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

The second phase is the qualitative, which is semi-structured interviews with subset of survey needed to examine users experienced and perceptions with cyber-security awareness training. Also, thematic analysis will be use analyse the interview transcripts. and to identify the recurring patterns and themes to cyber security training effectiveness, suggestions, and challenges. Also, use triangulation method to integrate the qualitative findings with quantitative results to provide a more holistic understanding of those factors influencing cybersecurity awareness training outcomes.

Lastly, an online interactive procedure developed to addresses the key themes. This will be an online and interactive training module which will be based on the findings from both qualitative and quantitative. Interactive features like simulations, quizzes, and case studies are incorporate to engage workers and to enhance the retention of knowledge.

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 choice, self-assessment, and scenario-based questions. The aim here is to establish baseline data on workers. Second is training program participation; in this case are the engagement levels. The aim here is to monitor workers’ participation.

# **IV. DATA PRESENTATION AND ANALYSIS**

## **Overview of the Problem**

Security Awareness Training (SAT) programs and procedures plays and important role in assisting organizations and companies mitigate the growing threats which are posted by the various cyber-attacks like insider threats, malware, and phishing. While the SAT programs aim at improving employees’ attitudes, behaviours, and knowledge toward cyber-security, its effectiveness remains an issue and challenging. As showcased in the literature review section, companies and organizations struggle to measure whether these programs lead to a practical improvement in incident response or even reduce cyber-security incidents or even a greater adherence to the cyber-security policies. Furthermore, a gap exists between the training efforts and the actual behaviour in workers, which leaves companies and organizations vulnerable despite their daily efforts to having a robust awareness campaign.

This chapter includes two major parts which are a document analysis (literature analysis) and a data analysis section. Literature review analysis, this involved, and evaluation of the academic journals and case studies carried out previously. The second section is a presentation of data and analysis from the data collected.

## **Data analysis and findings**

The aim of this analysis was to assess the effectiveness of SAT programs within an organization set-up. The data collected in this case was from 50 respondents via structured questionnaire. The questionnaire was divided into several sections which included demographic information, the pre-training assessment, employee behaviour, and post-training security questions. The data created in here enabled the project to analyse pre and post training effectiveness in improving awareness in cyber security along with the key metrics like phishing recognition improvements, updating habits, and passwords

### **Data and modelling approach**

As highlighted in the previous section a mixed methodology was utilized. In this case, the same was done where a mixed method approach for analysis was done. This was an integration of both qualitative and quantitative from the questionnaire. The quantitative data was derived from the respondents’ answers to closed-ended questions like frequency of password updates and phishing recognition, Qualitative responses like training types was also collected.

In this case the following was the modelling approach which was applied. First was the descriptive statistics which was done to provide the overall picture of the respondent demographics. Second was the comparative analysis which was done to compare both post and pre-training methods attitudes, behaviours, and knowledge. Lastly, was the data visualization modelling, this is the production of charts and graphs to identify the trends and at the same time interpret training effectiveness in line with the objectives of the study.

### **Results of Data analysis**

#### **Demographic Overview**

From the data collected the respondents ranged between the ages of 20 to 55 years with most of them being the ages of 30 to 40 years who were at sixty percent. Second was the gender where 55 percent were males and 45 percent being female. Lastly was the department where most of the respondents came from the IT department at 40 percent followed by the finance department at 25 percent, 20 percent being from the sales department and 15 percent from the operations.

#### **Pre-training vs. Post training security assessment**

#### First, the data collected for this study was from two major sections. First, is the pre-training data where the initial knowledge, attitudes, and behaviour towards cyber-security. Second was the post-training data where employees gave data on their perceived impact of the training on their behaviour and awareness. As indicated from the demographic data collected, the respondents were from various departments including operations, sales, procurement, finance, and IT. This ensured a diverse sample was collected. The key metrics included knowledge of common threats, phishing recognition capabilities, the likelihood of reporting suspicious activities, and the frequency of password updates.

Table 5.2.2a below is a data presentation in table of both pre-training and post training assessment based on the 50 questionnaire results.

Table 5.2.2a. Pre-training Assessment

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Category** | **Poor (n and %)** | | **Fair ((n and %)** | | **Good (n and %)** | | **Excellent ((n and %)** | |
| Cyber-security knowledge | 10 | 20% | 15 | 30% | 20 | 40% | 5 | 10% |
| Frequency of Password update | 5 | 10% | 10 | 20% | 20 | 40% | 15 | 30% |
| Phishing recognition ability | 12 | 25% | 20 | 10% | 12 | 25% | 6 | 10% |
| Frequency of Incident Reporting | 5 | 10% | 15 | 30% | 10 | 20% | 20 | 40% |

From the above table it is evident that the pre-training assessment provides insights into the workers cyber –security awareness before the training. From the table above it is evident that that majority of respondents either rated their cyber-security knowledge as being Good or Poor. This suggests that most of the employees have a basic understanding of cyber-security. Also, this suggests that a significant number of employees lacked that confidence of their knowledge.

When it comes to frequency of password update. The data collected indicates that only 30 percent who regularly update their passwords. This reflects a security gap which exists in most organizations. For phishing 25 percent rates their ability as Poor and only ten percent who considered themselves as people who are highly skilled in being able to identify phishing attacks. This shows a significant risk at identifying phishing related attacks. Lastly, from the table above and in terms of incident reporting frequency only 40 percent of the employees who always reported suspicious activities while ten percent indicating that they never reported any incident. The remaining 50 percent were spread between rarely and sometimes, indicating a room for improvement.

Table 5.2.2b: Post-training assessment

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Category | Poor (n and %) | | Fair **(n and %)** | | Good **(n and %)** | | Excellent **(n and %)** | |
| Cyber-security knowledge | 2 | 20% | 12 | 25% | 22 | 45% | 5 | 25% |
| Frequency of Password update | 2 | 5% | 8 | 15% | 8 | 15% | 15 | 65% |
| Phishing recognition ability | 5 | 10% | 15 | 30% | 22 | 45% | 6 | 15% |
| Frequency of Incident Reporting | 2 | 5% | 5 | 10% | 8 | 15% | 20 | 70% |

The table above showcases a clear improvement across all the four major areas as compared to the first one. In the category of cyber-security knowledge from the 50 respondents only 5 percent in this case two who are still rate their knowledge as poor. The same goes to the frequency of password update where the number of people who updated their passwords are usually often and one which rose from 30 percent that is 15 employees to a remarkable 32 workers. In terms of phishing recognition ability, the number of workers who rated themselves as poor dropped to ten percent, who were only five employees.

The project went ahead to develop a comparison graphs base on the data collected from the four cases.

A screenshot of a computer

Description automatically generated

Figure 5.2.2c: Cyber-security knowledge (Pre vs. Post training)

A screenshot of a computer

Description automatically generated

Figure 5.2.2d: Frequency of password update (Pre vs. Post training assessment)

A screenshot of a computer

Description automatically generated

Figure 5.2.2e: Phishing recognition improvement (Pre vs. Post assessment)

A screenshot of a computer

Description automatically generated

Figure 5.2.2f: Frequency Incident Frequency Reporting (Pre vs. Post training)

The above four graphs represent some of the key findings on security awareness based on fifty respondents. The cyber-security training awareness, the first graph shows a distribution where most of the response had a Good and Fair cyber-security knowledge. Nevertheless, after the security training awareness there was a significant increase in cyber-security knowledge were Excellent and Good increased significantly. The second graph shows that a substantial portion who reported updating their passwords rarely and sometimes. After the training, there was an increase and a shift towards often, showcasing that the training was in away successfully reinforced among the employees.

On the third graph, there was an improvement in the recognition of phishing. Post training data shows that 45 percent were now able to recognize phishing attempts. This was an increase from 25 percent, showcasing a remarkable improvement. Lastly, was on the incident response frequency. In here incident response improved considerably. This suggests a heightened responsibility and awareness towards company’s security.

# **IV. Online Interactive Training Portal Development**

## **Overview**

First from the previous chapter, the literature review section, there are three major case studies which were reviewed which were the SANS institute, the university of California, Berkely, and Xerox Corporation. These three organizations have implemented the SAT programs.

The key findings of the three case studies were first, the SANS institute case, the organization has developed what they have referred role specific modules to cater for various employees. According to the organization this ensures that the content is relevant to each role. All the general employees are always trained on recognizing a phishing mail and how to use secure communications. Second, the SAN cyber-security program emphasizes on the essence of tracking the effectiveness of their training. The SANs case demonstrates the essence of tailoring SAT programs as per the various employee’s roles.

The second case Xerox Corporation as reviewed from the previous section. One of the key findings is that the organization have employed a holistic and blended approach in training their employees. The organization have in a hands-on experience like phishing attack simulations which is followed by an online assessment. Also, they use employee feedback component for continuous feedback. Lastly was the UC Berkeley which utilizes a phishing simulation which is provided by measurable evidence of engagement.

Based on this, this project developed a sample and simulated online interactive security awareness training program. It is an interactive cyber-security online interactive portal where an individual can study on the various cyber-security programs. The portal was developed using PHP as the back-end programming language and HTML as the front-end language. The database utilized was from the XAMMP server which was used to store the database items.

## **System requirements**

The developed online interactive portal aims at enhancing user engagement by assisting users to be aware of the various cyber-security programs. The online interactive portal developed can be categorized into functional and non-functional requirements

### **Functional requirements**

*User registration and authentication of users*

Here users are required to register themselves with the portal and the login. Below are the interfaces of both register and login interface.

Register interface

A screenshot of a computer

Description automatically generated

Figure 4.2.1a: Register interface

A screenshot of a computer

Description automatically generated  
figure 4.2.1b: The login interface

**Cyber-security training dashboard**

Cyber-security awareness programs are the second interface which have been developed. Here users can start training. After login page, users are taken directly to the cyber-security awareness interface. Here users can start the process of cyber-security training. This is as shown by the interface shown below. Mainly, this page lists all the programs which are offered on the online interactive portal.

Figure 4.4a Screenshot of the training start session

A computer screen shot of a computer screen

Description automatically generated

Third functional requirement is the program interface. Here users can be able to start. After training able to do a quiz as per what they have trained and provide feedback about the interactive training. The interface is as shown by the page below

A screenshot of a computer

Description automatically generated

Figure 42.1d: Cyber-security training dashboard

By click of the start training program, users can view the sections and able to learn. This is as shown by the interface shown below

A screenshot of a computer

Description automatically generated

Figure 42.1c: Cyber-security training dashboard

Fourth functional requirement is that of start a quiz where users are asked quizzes as per the sub-topic they have trained. The user interface of the page is as shown below

A screenshot of a computer

Description automatically generated

Figure 42.1d: Cyber-security training dashboard: Quiz session

The last functional requirement is users being able to give feedback about their online interactive portal. The interface is as shown by the figure shown below

A screenshot of a computer

Description automatically generated

Figure 42.1e: Cyber-security training dashboard: feedback session

### **Non-functional requirements**

The online interactive portal designed has the following non-functional requirements. These are.

* Performance: The online interactive portal can load within three seconds on the user browser
* Security: Users can carry out their training without first login and providing their usernames and passwords. Also, the user data is protected using MD5 encryption standard. From example in the database, when a user inserts their password, it is protected from viewing the administrator. This is a shown by figure 12 below
* Usability: The portal is intuitive with a user-friendly interface
* Scalability: Lastly is that online interactive portal accommodates future growth both in terms of content and user based.

A screenshot of a computer

Description automatically generated

Figure 42.1f: Cyber-security training dashboard: Admin session

## **Architecture design**

The design comprises of front-end and back-end. This ensures a seamless integration of an online interactive experience by the users.

### **4.3.1 Front-end architecture**

* HTML/CSS: The styling and structure of the user interface was developed using CSS2 and HTML5 adhering to the current design standards
* Responsive design: A flexible grid layout and media queries were employed to ensure a media compatibility
* JavaScript framework: In this case various libraries were employed such as jQuery to enhance that interactivity like validation of the login and the register form.

### **Back-end architecture**

* A server-side framework: In this case PHP programming language was utilized. It provided that back-end interaction between the front and the database  
  Database: In this case, XAMMP database was utilizes to manage the user data, program contents, feedback, and quizzes
* The development tool utilized in this case was the visual studio code due to its versatility and a robust support for JavaScript and PHP

## **Purpose of the Online training portal**

The primary objective of this training is to educate users on the important topics of Data Protection and Information Security. This is accomplished through visually engaging infographics, allowing users to quickly grasp essential concepts. Additionally, the app includes an interactive quiz feature to let users evaluate and reinforce their understanding of the subject matter in an engaging way.

**Key Features and Sections**

The interface is structured into three main sections:

**1.** **Training Page:** The Training page is the main learning area, with easy-to-understand infographics that break down complex information. At the end, there’s a test where users can apply what they’ve learned and get a score to see how well they understood the material.

**2**. **Quiz Page**: The Quiz page lets users answer questions about Data Protection and Information Security. Users get a score based on how many answers they get right, helping them track their progress and see how much they’ve learned.

**3. Additional Resources**: This section provides links and information on external resources for users who want to deepen their knowledge. Users can access reputable sources and guides, ensuring they have a well-rounded understanding of the topics.

**Hosting and Cost Efficiency**

The online interactive portal is hosted on Google Cloud Run using the free tier, which provides reliable, scalable hosting at no extra cost. This setup makes the app available to users everywhere without any added expense. See link and screenshot below.

<https://training-app-jodgtg54tq-nw.a.run.app/>.

**IV. DISCUSSIONS**

The findings in this case provided a compelling evaluation of the effectiveness of cyber-security training awareness. The structured questionnaire presented in this case provided a robust framework for understanding the impact of security awareness currently provided. This chapter critically examines the data presented in the previous chapter and connects them to the research objectives while at the same time addressing the research objectives

## **Interpretation of the results**

The initial assessment of the data presented and analysis presented in the previous chapter reveals important gaps which underscores the need for a comprehensive training. Additionally, the post training data presented in the previous chapter reveals a substantial improvement across various metrics emphasizing the effectiveness of cyber-security awareness training programs

## **Connecting to the literature review**

The findings of this research project are consistent with the literature on the effective of security awareness training programs and connect them directly to the three case studies. First is on SANS Institute case, first the findings that improvement in phishing recognition mirrors the outcome of the SANs institute case. From the case the organization enhanced employee ability to recognize phishing emails via small-burst trainings sessions. The same is reflected in the research findings on post training assessment where security training resulted to improved employee behavior. On the same case as listed in the case studies review, SANs emphasizes on the need of post training assessments of employees to have feedback.

On the second case study, password management behaviours from the data presented parallels with Xerox Corporation cyber-security awareness program. From the Xerox case, the organization utilizes interactive and gamification platforms to encourage a better hygiene management of passwords.

Lastly, the University of California, Berkeley increasingly viewed cyber security training as a shared responsibility. The same is observed from the data presented where most of the employees who presented their view security as a mandatory training or what was referred in the questionnaire as shared responsibility.

# VI. Conclusion.

This report examines the effectiveness of employee training in information security. The findings indicate a need for ongoing improvement and enhancement of security awareness training programs. It recognizes the importance of security awareness and emphasizes that such initiatives contribute to building organizational resilience rather than resistance. To mitigate the risk of human error, it ‘recommended that training and awareness programs be customized to align with individual’s role, knowledge, and skills. This customization should be a continuous process, considering the evolution of security knowledge, employee turnover, and the shifting demands of various roles.

The speed at which awareness is created does not depend on the value of security awareness, but rather on how well it is integrated with the overarching objective of the organization, its communication methods, compliance mechanisms, and employee learning capabilities.

Studies on the psychology of security behavior and awareness emphasize the need for ongoing planning and enhancement of training to effectively change behaviors. Theoriesal theories indicate that the success of these training initiatives depends on an individual's readiness to adapt. Therefore, fostering a successful security culture necessitates an organizational commitment to security. Organizations now seek to cultivate a security culture that goes beyond mere awareness and compliance. Integrating information security into daily planning processes is vital, it needs embedment at all levels of execution. To strengthen security culture within organizations through training, a more holistic strategy involving human resources is essential, considering both business and psychological perspectives. While existing literature has suggested strategies for a unified security approach, further research is needed to optimize its implementation and impact in organizations. Adopting a behavioral perspective has significant implications for future research and improved practices in the information security field.

# **References**

Alkhalil Z, Hewage C, Nawaf L and Khan I (2021) Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. *Front. Computer. Sci.* 3:563060. Doi: 10.3389/fcomp.2021.563060

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I., (2021). Phishing attacks: A recent comprehensive study and a new anatomy. Frontiers in Computer Science. [frontiersin.org](https://www.frontiersin.org/journals/computer-science/articles/10.3389/fcomp.2021.563060/full?ref=hackernoon.com)

Andrew S. (2023). The cybersecurity risks caused by human error and how to avoid them. Available at <https://www.readyworks.com/blog/the-cybersecurity-risks-caused-by-human-error-and-how-to-avoid-them>. (Accessed 20 June 2024.

Baburajan, V., e Silva, J.D.A. and Pereira, F.C., (2022). Open vs closed-ended questions in attitudinal surveys–Comparing, combining, and interpreting using natural language processing. Transportation research part C: emerging technologies, 137, p.103589. [[PDF]](https://arxiv.org/pdf/2205.01317)

Calder, A., (2023). ISO 27001/ISO 27002: A guide to information security management systems

Ciudin, P., Goia, H.Ș. and Popișter, F., (2024), March. Implementation of Human Gestures in the Control of Collaborative Robots. In International Scientific-Technical Conference MANUFACTURING (pp. 27-42). Cham: Springer Nature Switzerland. [[HTML]](https://link.springer.com/chapter/10.1007/978-3-031-56467-3_3)

Cybsafe (2023). Security Awareness: 7 reasons why security awareness training is important in 2023. Available at <https://www.cybsafe.com/blog/7-reasons-why-security-awareness-training-is-important/>. Accessed 07 February 2024.

Darem, A. (2021). Anti-Phishing Awareness Delivery Methods. Engineering, Technology & Applied Science Research, 11(6), 7944–7949. <https://doi.org/10.48084/etasr.4600>.

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>.

Griffin, L., (2021). The Effectiveness of Cybersecurity Awareness Training in Reducing Employee Negligence Within Department of Defense (DoD) Affiliated Organizations-Qualitative …. [[HTML]](https://search.proquest.com/openview/3f9ba5f2497720820c5c758bc6118a2e/1?pq-origsite=gscholar&cbl=18750&diss=y)

Gupta, P., Srinivasan, B., Balasubramaniyan, V., and Ahamad, M. (2015). “Phoneypot: data-driven understanding of telephony threats,” in Proceedings 2015 network and distributed system security symposium, (Reston, VA: Internet Society),8–11.doi:10.14722/ndss.2015.23176.

Hart, S., Margheri, A., Paci, F., & Sassone, V., (2020). Riskio: A serious game for cyber security awareness and education. Computers & Security. [soton.ac.uk](https://eprints.soton.ac.uk/441632/1/Riskio_A_Serious_Game_for_Cyber_Security_Awareness_and_Education.pdf)

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>

Hornet security (2023) 1 In 3 Organisations does not provide any cybersecurity training to remote workers. Available at <https://www.hornetsecurity.com/en/press-releases/1-in-3-organizations-does-not-provide-any-cybersecurity-training-to-remote-workers/>

Husband, G., (2020). Ethical data collection and recognizing the impact of semi-structured interviews on research respondents. Education Sciences.

IBM. (2019). IBM Study Shows Data Breach Costs on the Rise; Financial Impact Felt for Years - Jul 23, 2019. IBM Newsroom. <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). 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>.

Jampen, D., Gür, G., Sutter, T. and Tellenbach, B., (2020) *please cite it as Jampen et al.* Don’t click towards an effective anti-phishing training. A comparative literature review. Human-centric Computing and Information Sciences, 10(1), p.33. [springer.com](https://link.springer.com/content/pdf/10.1186/s13673-020-00237-7.pdf)

Khando K, Gao S, Islam S M, Salman A (2021). Computers & security, Elsevier. Enhancing employee’s information security awareness in private and public organisations: A systematic literature review. [sciencedirect.com](https://www.sciencedirect.com/science/article/pii/S0167404821000912).

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

Lance S (2023) SANS: Security Awareness Report: Managing Human Risk. Available at <https://www.sans.org/blog/sans-2023-security-awareness-report-managing-human-risk/?msc=SAR23-Promo-Homepage> accessed 25 June 2024

McIlwraith A (2021). Taylorfrancis.com. Information security and employee behaviour: how to reduce risk through employee education, training, and awareness. [[HTML]](https://www.taylorfrancis.com/books/mono/10.4324/9780429281785/information-security-employee-behaviour-angus-mcilwraith)  
Cited by **187**

Palanisamy R. Norman A. A. And Kiah L. M. (2020): BYOD Policy Compliance: Risk and Strategies in Organizations. Journal of Computer Information Systems, DOI: 10. 1080/08874417.2019.1703225. Available at https://doi.org/10. 1080/08874417.2019.1703225.

Parthy, P.P. and Rajendran, G. (2019) ‘Identification and prevention of social engineering attacks on an enterprise,’ in 2019 International Carnahan Conference on Security Technology (ICCST), pp. 1–5. Available at: <https://doi.org/10.1109/CCST.2019.8888441>. (Accessed, 10 January 2024).

Rodrigues, G.A.P., Serrano, A.L.M., Vergara, G.F., Albuquerque, R.D.O. and Nze, G.D.A., (2024). Impact, Compliance, and Countermeasures in Relation to Data Breaches in Publicly Traded US Companies. Future Internet, 16(6), p.201. [mdpi.com](https://www.mdpi.com/1999-5903/16/6/201/pdf)

Salisbury, M. D., (2024). The Role of the Corporate Trainer: Influence on Employee Behavior and Identity. [[HTML]](https://search.proquest.com/openview/6cee72eb95fcbacb1caee5d2f7aeb9f2/1?pq-origsite=gscholar&cbl=18750&diss=y)

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>

The Open University (2012) Module T802: Preparing for research. Available at <https://learn2.open.ac.uk/mod/oucontent/view.php?id=2237689&section=1.3>.

University of California. (n.d.). UC Cyber Security Awareness Fundamentals | People & Culture. Hr.berkeley.edu. Available at <https://hr.berkeley.edu/grow/grow-your-skills/useful-learning-links/foundational-skills-required-training/uc-cyber-security#:~:text=This%20interactive%20Cyber%20Security%20Awareness>. Accessed 28 March 2024

University of California (2024) UC Cyber Risk program report. Available at <https://security.ucop.edu/files/documents/2023-annual-report.pdf>. Accessed 25 October 2024

Verizon. (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>.

Younis, Y.A. and Musbah, M., 2020, September. A framework to protect against phishing attacks. In Proceedings of the 6th International Conference on Engineering & MIS 2020 (pp. 1-6). [[HTML]](https://dl.acm.org/doi/abs/10.1145/3410352.3410825)

# **Appendices**

## **Appendix 1: Planning and scheduling**

The table below details the planning and scheduling of this research project and is subject to refinement.

Figure 6a: Schedule and research plan.

|  |  |  |  |
| --- | --- | --- | --- |
| Task ID | Description | Duration | Progress |
| Stage 0.0 | Research Synopsis Preparation/Submission | 37 | 100% |
| Stage 0.1 | Preparation before the start date | 55 | 100% |
| Stage 1.0 | Developing Research Proposal | 11 | 100% |
| Stage 1.1 | Synopsis submission and approval | 10 | 100% |
| Stage 1.2 | Iterations of the research proposal | 35 | 100% |
| Stage 1.3 | Easter holiday (church & family engagement | 5 | 100% |
| Stage 1.3 | TMA 01 preparation and submission | 8 | 100% |
| Stage 2.0 | Focusing on the literature review | 17 | 100% |
| Stage 2.1 | Going back to Refining Topic & Objectives | 12 | 100% |
| Stage 2.2 | Prepare and submit TMA 02 | 18 | 100% |
| Stage 3.0 | Focusing on the Methodology by reading | 22 | 100% |
| Stage 3.1 | prepare and design questionnaire (15 question) | 10 | 100% |
| Stage 3.2 | send survey questionnaire online and by email | 5 | 100% |
| Stage3.3 | Going back to Refine Case Study, Method & Lit. | 10 | 100% |
| Stage 3.4 | Online Interactive Portal Development, | 11 | 100% |
| Stage 3.5 | TMA03 preparation | 32 | 100% |
| Stage 3.6 | TMA 03 review and submission | 4 | 100% |
| Stage 4.0 | Cont. research, and review Feedback from tutor | 9 | 100% |
| Stage 4.1 | Online Interactive Portal Development Refined | 10 | 100% |
| Stage 4.2 | Data collection, cont. work | 10 | 100% |
| Stage 4.3 | Data analysis and representation | 12 | 100% |
| Stage4.3.1 | Data analysis and findings | 7 | 100% |
| Stage4.3.2 | Results of Data analysis | 8 | 80% |
| Stage 4.4 | TMA04 Preparation | 7 | 100% |
| Stage 4.5 | TMA04 Review/submission | 2 | 100% |
| Stage 5.0 | Completing research, design online interactive | 41 | 0% |
| Stage 5.1 | Christmas and New year holiday TMA04 review | 9 | 0% |
| Stage 5.2 | Recommendation and dissertation write up | 30 | 0% |
| Stage 5.3 | Dissertation review & proofread | 8 | 0% |
| Stage 5.4 | Dissertation submission | 2 | 0% |

## **Appendix 2: Gantt Chart Planning and Scheduling table**

A screenshot of a computer

Description automatically generated

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **PROJECT NAME** | **START DATE** | **END DATE** | **Duration** |  |
|  | MSc in Computing and Network (T802) | 01/11/2023 | 12/02/2025 |  |  |
| **Task ID** | **Description** | **Start Date** | **End Date** | **Duration** | **Progress** |
| Stage 0.0 | Research Synopsis Preparation/Submission | 01/11/2023 | 07/12/2023 | 37 | 100% |
| Stage 0.1 | Preparation before the start date | 08/12/2023 | 31/01/2024 | 55 | 100% |
| Stage 1.0 | Developing Research Proposal | 01/02/2024 | 11/02/2024 | 11 | 100% |
| Stage 1.1 | Synopsis submission and approval | 12/02/2024 | 21/02/2024 | 10 | 100% |
| Stage 1.2 | Iterations of the research proposal | 22/02/2024 | 27/03/2024 | 35 | 100% |
| Stage 1.3 | Easter holiday (church & family engagement | 28/03/2024 | 01/04/2024 | 5 | 100% |
| Stage 1.3 | TMA 01 preparation and submission | 02/04/2024 | 09/04/2024 | 8 | 100% |
| Stage 2.0 | Focusing on the literature review | 10/04/2024 | 27/04/2024 | 17 | 100% |
| Stage 2.1 | Going back to Refining Topic & Objectives | 28/04/2024 | 10/05/2024 | 12 | 100% |
| Stage 2.2 | Prepare and submit TMA 02 | 11/05/2024 | 28/05/2024 | 18 | 100% |
| Stage 3.0 | Focusing on the Methodology by reading | 29/05/2024 | 20/06/2024 | 22 | 100% |
| Stage 3.1 | prepare and design questionnaire (15 question) | 21/06/2024 | 30/06/2024 | 10 | 100% |
| Stage 3.2 | send survey questionnaire online and by email | 01/07/2024 | 05/07/2024 | 5 | 100% |
| Stage3.3 | Going back to Refine Case Study, Method & Lit. | 06/07/2024 | 16/07/2024 | 10 | 100% |
| Stage 3.4 | Online Interactive Portal Development, | 17/07/2024 | 27/07/2024 | 11 | 100% |
| Stage 3.5 | TMA03 preparation | 28/07/2024 | 28/08/2024 | 32 | 100% |
| Stage 3.6 | TMA 03 review and submission | 29/08/2024 | 01/09/2024 | 4 | 100% |
| Stage 4.0 | Cont. research, and review Feedback from tutor | 02/09/2024 | 20/09/2024 | 9 | 100% |
| Stage 4.1 | Online Interactive Portal Development Refined | 21/09/2024 | 30/09/2024 | 10 | 100% |
| Stage 4.2 | Data collection, cont. work | 01/10/2024 | 10/10/2024 | 10 | 100% |
| Stage 4.3 | Data analysis and representation | 11/10/2024 | 22/10/2024 | 12 | 100% |
| Stage  4.3.1 | Data analysis and findings | 21/10/2024 | 27/10/2024 | 7 | 100% |
| Stage  4.3.2 | Results of Data analysis | 28/10/2024 | 03/11/2024 | 8 | 80% |
| Stage 4.4 | TMA04 Preparation | 04/11/2024 | 10/11/2024 | 7 | 100% |
| Stage 4.5 | TMA04 Review/submission | 11/11/2024 | 12/11/2024 | 2 | 100% |
| Stage 5.0 | Completing research, design online interactive | 13/11/2024 | 23/12/2024 | 41 | 0% |
| Stage 5.1 | Christmas and New year holiday TMA04 review | 24/12/2024 | 01/01/2025 | 9 | 0% |
| Stage 5.2 | Recommendation and dissertation write up | 02/01/2025 | 01/02/2025 | 30 | 0% |
| Stage 5.3 | Dissertation review & proofread | 02/02/2025 | 09/02/2025 | 8 | 0% |
| Stage 5.4 | Dissertation submission | 10/02/2025 | 11/02/2025 | 2 | 0% |
|  |  |  |  |  |  |
|  | **NOTE:** The area with red represent work done due to the life circle model used | | |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

[T802 research Gantt chart TMA 04.xlsx](https://1drv.ms/x/s!AtKndxCfXpSyug8khD_bp81JCrCy?e=bfwx99)

## **Appendix 3: Progress to date.**

This project has experience changes using iterative lifecycle model. First, the topic was refined due to tutor feedback to “*An investigation and evaluation into the effectiveness of security awareness training process in organisations.”* The schedule plan keep updated as the work progresses. See table 7.1

Table 7.1: Planned progress to date.

|  |  |  |  |
| --- | --- | --- | --- |
| **Task ID** | **Description** | Duration | **Progress** |
| Stage 0.0 | Research Synopsis Preparation/Submission | 37 | 100% |
| Stage 0.1 | Preparation before the start date | 55 | 100% |
| Stage 1.0 | Developing Research Proposal | 11 | 100% |
| Stage 1.1 | Synopsis submission and approval | 10 | 100% |
| Stage 1.2 | Iterations of the research proposal | 35 | 100% |
| Stage 1.3 | Easter holiday (church & family engagement | 5 | 100% |
| Stage 1.3 | TMA 01 preparation and submission | 8 | 100% |
| Stage 2.0 | Focusing on the literature review | 17 | 100% |
| Stage 2.1 | Going back to Refining Topic & Objectives | 12 | 100% |
| Stage 2.2 | Prepare and submit TMA 02 | 18 | 100% |
| Stage 3.0 | Focusing on the Methodology by reading | 22 | 100% |
| Stage 3.1 | prepare and design questionnaire (15 question) | 10 | 100% |
| Stage 3.2 | send survey questionnaire online and by email | 5 | 100% |
| Stage3.3 | Going back to Refine Case Study, Method & Lit. | 10 | 100% |
| Stage 3.4 | Online Interactive Portal Development, | 11 | 100% |
| Stage 3.5 | TMA03 preparation | 32 | 100% |
| Stage 3.6 | TMA 03 review and submission | 4 | 100% |
| Stage 4.0 | Cont. research, and review Feedback from tutor | 9 | 100% |
| Stage 4.1 | Online Interactive Portal Development Refined | 10 | 100% |
| Stage 4.2 | Data collection, cont. work | 10 | 100% |
| Stage 4.3 | Data analysis and representation | 12 | 100% |
| Stage4.3.1 | Data analysis and findings | 7 | 100% |
| Stage4.3.2 | Results of Data analysis | 8 | 80% |
| Stage 4.4 | TMA04 Preparation | 7 | 100% |
| Stage 4.5 | TMA04 Review/submission | 2 | 100% |
| Stage 5.0 | Completing research, design online interactive | 41 | 0% |
| Stage 5.1 | Christmas and New year holiday TMA04 review | 9 | 0% |
| Stage 5.2 | Recommendation and dissertation write up | 30 | 0% |
| Stage 5.3 | Dissertation review & proofread | 8 | 0% |
| Stage 5.4 | Dissertation submission | 2 | 0% |

As contained in Figure 6.1 Gantt Chart Planning and Scheduling table, stage 1 to stage 4 is in 100% completion rate. The planning and scheduling define the travel of this project, updated based on research development. The fourth case study: Maersk case study, removed due to its outdated source. The objectives reduced from 5 to 4.

The first challenge was getting the relevant literature and case studies. Lot of literature where reviewed. It has been a challenge getting data of the training conducted by Case study 2: Xerox Corporation and that of university of California without login details to access their database. Using PROMPT analysis, the relevant literature where obtained. After numerous feedback and advice from tutor a clear understanding of what is required on Aim, objectives, methods, tasks, and deliverables were achieved. The biggest challenge is my organization losing contract and staff handed over to a new organization after planning my questionnaire survey plan.

Survey questionnaire developed and sent to target respondents via email and online. Fifteen questions were designed and sent across. Here is a link to the online survey questionnaire, <https://forms.gle/MCsQ9dmtxb9QtN8BA>.

Data collected, analyzed, and presented. As presented in stage 4 of the project. Online iteratives designed and presented as options 1 and 2. A portal that allows users to register and login to access the training. Details of completed application given in stage 4 and 5. As stated in TMA 03, the challenges encountered in the survey process, such as losing the intended respondent, was resolve meet with other respondents and the decision to go online. As presented in stage 5. The data was collected with fifty respondents and analyzed. The final stage is writing as dissertation.

As earlier stated, an online iterative training portal developed recommended to ease the cost of training program and make awareness training more interactive for users. Below is a link undergoing development of such training and stage 4 of this paper deals with option one**. (Online Interactive Portal Development**). Option is more technical and need to log in to have access. But option two when developed can be deploy organisation who want to cut cost or for quick awareness regular training. And it can be sent as link to employee**.**

<https://training-app-jodgtg54tq-nw.a.run.app/>.

***Quiz***

[*https://forms.gle/gdZs76i2bV9HQDEL9*](https://forms.gle/gdZs76i2bV9HQDEL9)

## **Appendix 4: More on Online iterative portal.**

Database

A screenshot of a computer

Description automatically generated

**Figure 1:1 Online iterative: phpMyAdmin**

A screen shot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Training portal

A screenshot of a computer

Description automatically generated

Figure 1:3 start page

A screenshot of a quiz

Description automatically generated

Figure 1;4 Quiz page

**Appendix 2: Online Training second option**

**A screenshot of a computer

Description automatically generated**

Figure 2:1. Online Training Option 2. Start Training page

A screenshot of a web page

Description automatically generated

Figure 2:2 Training and information page

A screenshot of a quiz

Description automatically generated

Figure 2:3 Quiz section

A screenshot of a computer

Description automatically generated

Figure 2:4 Additional informational secti

## **Appendix 5: Survey questionnaire**

Here is the link to Survey questionnaire: <https://forms.gle/MCsQ9dmtxb9QtN8BA>

**Topic: *An investigation and evaluation into the effectiveness of security awareness training process in organisations.***

**Survey Questionnaire: MSc Research Project**

A Survey questionnaire designed to carry out an investigation into the effectiveness of security awareness training and evaluate whether the process makes any measurable differences in the security posture of any organization.  
This survey is aimed at anyone over the age of 18, employees of any organization, IT professional and management of any organization with access to company data.  
  
The purpose of this survey is to gather information by investigating the effectiveness of security awareness training and evaluate whether the process makes any measurable differences in the security posture of any organization.  
The data collected will be used for an Open University MSc in Computing research project.  
  
No personally identifiable information will be collected or stored as part of this survey.  
You can stop the survey at any time, and partly completed surveys will not be recorded. If you do not wish to answer any of the questions, please choose the option marked "Prefer not to say".  
  
The questionnaire will take about 5-7 minutes to complete. If you would like to receive a copy of the summary results once the survey is complete, please email...  
**Eligibility**  
To participate in this survey, individuals must be 18 years or older.

NOTE

IF you wish not to participate in this survey please discontinue. By continuing show you’ve given your consent.

**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?





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 |  |

**Appendix 4: Quiz: Information Security Awareness Model updated**

Here is the link:

[https://forms.gle/gdZs76i2bV9HQDEL9](https://emea01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fforms.gle%2FgdZs76i2bV9HQDEL9&data=05%7C02%7C%7Caaef0b45df6244668b8008dcf2c90d3c%7C84df9e7fe9f640afb435aaaaaaaaaaaa%7C1%7C0%7C638652192527379182%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=v7q5Z5XKECoMgaOQoQjbiG4vvPnleYOAuMqQ8h85tKM%3D&reserved=0)

*I’ve checked Quiz in link above. Please need to give score and feedback to each response.*

A computer screen shot of a computer screen

Description automatically generated

**Quiz: Information Security Awareness Model updated**

Q1:

The Information Security Password policy states that passwords for the organisation must have an expiration period. How long is that period?

According to the Information Security Password policy, organisation passwords must be set to expire after how long?

Select one:

organisation passwords never expire

90 days

Every time I sign in

6 months

Q2:

The organisation possesses various kinds of information. Which two of the following statements accurately reflect the types of information that require protection?

Please choose one or more:

We need to protect company’s commercial information (contracts, bids, tenders, etc)

Personal information about any living person needs to be protected

Only personal information about staff and customer needs to be protected

Organisation sales report data does not need security protection

Company financial information does not need to be protected

Q3:

Why is information security important? (Select all that apply)

Select one or more:

To protect Organisation financial and personal information

To support staff to work securely

To protect organisation, staff, and customer information

To protect organisation information and systems

Q4:

If you receive an email that you think might be a phishing attempt and you accidentally click on the link that leads you to a website, but you close the browser without engaging with anything on the page, what should your next steps be?

Select one:

Report the message as Phishing and inform Information Security on the action you took

Forward the message on to a colleague to ask them whether they also received it

Nothing, you did not interact with any content on the website, so there is no risk

Delete the email and ignore it

Q5:

Is the following statement True or False?

To protect yourself from phishing attacks, always refrain from opening unexpected email attachments from unfamiliar senders. 

Select one:

True

False

Q6:

Is the following statement true or false?

Since my workplace is safe, I can leave customer information on my desk when I'm not present.

Select one:

True

False

Q7:

What steps should you take when you step away from your computer for five minutes in your regular work environment? (choose one response)

Select one:

Leave your computer unlocked, in case anyone else wants to use it remotely

Shut down and unplug the computer

Lock your computer screen when you leave it unattended

Shut down your computer screen and leave your password under the keyboard

Q8:

Who is responsible for information security at the Company?

Select one:

The Data Protection team

Organisation Communications team

All staff

The Data Insights team

Q9:

You get an email containing a link that seems legitimate, so you decide to click on it. Once you arrive at the webpage, you recognize that this is a phishing scam.

Select one:

If I didn't enter any credentials, there is no security risk

This needs to be reported - the web site could have infected my PC

Q10:

On the floor you find a USB drive that is not yours, what should you do?

Select one:



Plug the USB drive into your computer and navigate the files to try and find the owner as they may require it for an important piece of company work



Post a notice on the Company intranet reporting the lost USB drive and leave your contact details



Leave the USB drive on the floor for someone else to deal with in due course



Pick up the USB drive and lock it away and contact Information Security

**Glossary.**

**CIA PRINCIPLE**: - The CIA (confidentiality, integrity, availability) triad is a widely used information security model that can guide an organization’s efforts and policies aimed at keeping its data secure.

**EC-COUNCIL**: - EC-council is a company that offers various certification, education, training, and service in the IT Security field.

**CompTIA Security** :- The Computing Technology Industry Association, more commonly known as CompTIA, is an American non-profit [trade association](https://www.bing.com/ck/a?!&&p=3bc3c149982c0b57JmltdHM9MTcyNDU0NDAwMCZpZ3VpZD0wOWQ4MWMwNy00ZDMyLTYwZGUtMWZkNi0wODdmNGNkMjYxOGQmaW5zaWQ9NTU5MA&ptn=3&ver=2&hsh=3&fclid=09d81c07-4d32-60de-1fd6-087f4cd2618d&u=a1L3NlYXJjaD9xPUluZHVzdHJ5JTIwdHJhZGUlMjBncm91cCUyMHdpa2lwZWRpYSZmb3JtPVdJS0lSRQ&ntb=1) that issues [professional certifications](https://www.bing.com/ck/a?!&&p=e2c438824216ffc4JmltdHM9MTcyNDU0NDAwMCZpZ3VpZD0wOWQ4MWMwNy00ZDMyLTYwZGUtMWZkNi0wODdmNGNkMjYxOGQmaW5zaWQ9NTU5MQ&ptn=3&ver=2&hsh=3&fclid=09d81c07-4d32-60de-1fd6-087f4cd2618d&u=a1L3NlYXJjaD9xPVByb2Zlc3Npb25hbCUyMGNlcnRpZmljYXRpb24lMjB3aWtpcGVkaWEmZm9ybT1XSUtJUkU&ntb=1) for the [information technology](https://www.bing.com/ck/a?!&&p=43c179ab256cc6c2JmltdHM9MTcyNDU0NDAwMCZpZ3VpZD0wOWQ4MWMwNy00ZDMyLTYwZGUtMWZkNi0wODdmNGNkMjYxOGQmaW5zaWQ9NTU5Mg&ptn=3&ver=2&hsh=3&fclid=09d81c07-4d32-60de-1fd6-087f4cd2618d&u=a1L3NlYXJjaD9xPUluZm9ybWF0aW9uJTIwdGVjaG5vbG9neSUyMHdpa2lwZWRpYSZmb3JtPVdJS0lSRQ&ntb=1) (IT) industry. It considered one of the IT industry's top trade associations.

**CISSP PROGRAM**: - The Certified Information Systems Security Professional (CISSP) is an advanced certification for IT and cybersecurity professionals12345. It demonstrates their ability to design, implement, and manage an enterprise cybersecurity program. CISSP validates deep technical and managerial knowledge and experience in securing an organization's data and overall security posture.

**IOT**: - The Internet of Things (IoT) refers to a network of physical devices, vehicles, appliances, and other physical objects embedded with sensors, software, and network connectivity, allowing them to collect and share data.

AI: - Artificial intelligence (AI), in its broadest sense, is intelligence exhibited by machines, particularly computer systems.

**MYSQL:** This is an open-source relational database management system.

**HTML:** a hypertext markup language is the standard markup language for documents. designed to displayed in a web browser.

**PHP:** Hypertext Processor is a general=purpose scripting language and interpreter freely available in the web.

**SAT**: Security Awareness Training

**HIPAA:** Health Insurance Portability and Accountability Act. Requires organizations work with protected health information (PHI) to implement and follow physical, network, and process security measures.