

https://dspace.org/

Investigating online learning and its role in addressing the cybersecurity skills shortage in South Africa

Kgosiatsela, Lefa

2023
University of the Witswatersrand, Johannesburg
https://hdl.handle.net/10539/38499

Downloaded from a DSpace repository. https://dspace.org/

Investigating online learning and its role in addressing the cybersecurity skills shortage in South Africa

Lefa Kgosiatsela

2412173

Email: 2412173@students.wits.ac.za Mobile: 071 860 9702

A research proposal submitted to the Faculty of Commerce, Law and Management, University of the Witwatersrand, in partial fulfilment of the requirements for the degree of Master of Management in the field of Digital Business

Johannesburg, 2023

KEYWORDS

Online Learning, Cybersecurity, Skills, Information Security, South Africa, Training, Capture-the-flag

ABSTRACT

This study explores the pivotal role of online learning in addressing the shortage of cybersecurity skills within the South African financial services sector. The study investigates the preferred learning formats of cybersecurity professionals, scrutinizes the strengths and weaknesses of online learning, and evaluates its efficacy in imparting cybersecurity skills. Emphasis is placed on the principles of attention, retention, and motivation in cybersecurity training, focusing on their implications for different learning formats.

The decision to use a qualitative approach was influenced by the research questions, data requirements, and theoretical framework. A cross-sectional research design was chosen for its suitability in answering the research questions efficiently, considering the time constraints and the need for broad coverage in the complex field of cybersecurity. The advantages of this design include speedy data collection, simplicity in analysis, and suitability for exploratory research. Semi-structured interviews, conducted through Microsoft Teams, were employed for data collection from a sample of ten cybersecurity professionals, selected through a combination of purposive and snowball sampling methods. The interviews, comprising 16 open-ended questions organised into four sections, aimed to explore participant preferences, critical factors for successful online learning, and the efficacy of online learning in imparting cybersecurity skills. Thematic Content Analysis (TCA) was employed for data analysis, involving the organization of data, identification of common themes, and the interpretation of findings.

Online learning emerges as a flexible and accessible avenue for acquiring cybersecurity skills and knowledge. Despite its advantages, careful attention must be given to addressing potential drawbacks stemming from the absence of physical interaction and engagement. Instructors play a pivotal role in mitigating these challenges by incorporating interactive discussions, offering timely feedback, and fostering a sense of community among learners. The evaluation of online learning effectiveness should prioritize factors such as retention and practical skill application. Online platforms can contribute to this by providing diverse resources and tools. Success in online learning hinges on self-regulation

and time management skills, underscoring the importance of adequate support and tools within the online learning environment. In essence, online learning holds the potential to motivate cybersecurity professionals, fostering not only skill development but also a lasting enthusiasm for lifelong learning.

The research revealed distinct impacts of various training formats—physical on-the-job training, physical classroom training, and online training—on attention and engagement levels. Participants exhibited diverse preferences, with the majority favouring online self-paced and physical classroom training. Moreover, the study underscored the critical role of retention in cybersecurity training, emphasising the necessity for professionals to retain and recall knowledge and skills for effective application, necessitating continuous training to match the rapidly evolving nature of the field. Finally, the principle of motivation emerged as a key factor, indicating that participants driven to learn and apply their skills are more likely to excel in the cybersecurity field, as evidenced by their active participation in multiple training programs and specific format preferences.*Keywords: Online learning, Cybersecurity, Training*

TABLE OF CONTENTS

LIST OF FIGURES viii

LIST OF ACRONYMS ix

CHAPTER 1. INTRODUCTION 10

1.1 STATEMENT OF PURPOSE 10
1.2 BACKGROUND OF THE STUDY 10
1.3 RESEARCH PROBLEM 12
1.4 RESEARCH QUESTIONS 13
1.5 RATIONALE 13
1.6 DELIMITATIONS OF STUDY 14
1.7 DEFINITION OF TERMS 15
1.8 ASSUMPTIONS 15

CHAPTER 2. LITERATURE REVIEW AND THEORETICAL FRAMEWORK 16

2.1 INTRODUCTION 16
2.2 DEFINITION OF TOPIC OR BACKGROUND DISCUSSION 16
2.3 WHAT FORMAT OF LEARNING DO CYBERSECURITY PROFESSIONALS PREFER? 19
2.3.1 ON-THE-JOB TRAINING 19
2.3.2 CLASSROOM-STYLE TRAINING 19
2.3.3 ONLINE LEARNING 20
2.3.4 PROPOSITION 1 21
2.4 WHAT ARE SOME OF THE KEY CONSIDERATIONS FOR ONLINE LEARNING? 21
2.4.1 QUALITY, LOW RETENTION, NEED FOR ENGAGEMENT 21
2.4.2 PROPOSITION 2 21
2.5 IS ONLINE LEARNING EFFECTIVE AT TEACHING CRITICAL CYBERSECURITY SKILLS? 22
2.5.1 PROPOSITION 3 22
2.6 ANALYTICAL FRAMEWORK 22
2.6.1 THEORETICAL FRAMEWORK 22
2.6.2 CONCEPTUAL FRAMEWORK 23
2.6.3 PROPOSITION 1 24
2.6.4 PROPOSITION 2 24
2.6.5 PROPOSITION 3 25

CHAPTER 3. RESEARCH METHODOLOGY 26

3.1 RESEARCH APPROACH 26

3.2 Research design 27
3.3 Data collection methods 28
3.4 Population and sample 28
3.4.1 Population 28
3.4.2 Sample 29
3.5 The research instruments 29
3.6 Data Collection 30
3.7 Data analysis strategies and interpretation 30
3.8 Quality Assurance 31
3.8.1 Transferability 31
3.8.2 Credibility 31
3.8.3 Dependability 32
3.9 Ethical considerations 32

CHAPTER 4. PRESENTATION OF DATA 33

4.1 Data Collection 33
4.1.1 Introduction 33
4.1.2 Research Question 1 34
4.1.3 Research Question 2 35
4.1.4 Research Question 3 37

CHAPTER 5. ANALYSIS & FINDINGS 39

5.1 Introduction 39
5.2 Bandura's Social Learning Construct – Attention 40
5.2.1 Which learning format do cybersecurity professionals prefer? 40
5.2.2 What are the strengths and weaknesses of online learning? 42
5.2.3 Is Online learning effective at teaching cybersecurity skills? 43
5.3 Bandura's Social Learning Construct – Retention 44
5.3.1 Which learning format do cybersecurity professionals prefer? 44
5.3.2 What are the strengths and weaknesses of online learning? 45
5.3.3 Is Online learning effective at teaching cybersecurity skills? 45
5.4 Bandura's Social Learning Construct – Reproduction 46
5.4.1 Which learning format do cybersecurity professionals prefer? 46
5.4.2 What are the strengths and weaknesses of online learning? 47
5.4.3 Is Online learning effective at teaching cybersecurity skills? 47
5.5 Bandura's Social Learning Construct – Motivation 48
5.5.1 Which learning format do cybersecurity professionals prefer? 48
5.5.2 What are the strengths and weaknesses of online learning? 49
5.5.3 Is Online learning effective at teaching cybersecurity skills? 50
5.6 Conclusion 51

CHAPTER 6. CONCLUSION 52

6.1 Introduction 52
6.2 Key Takeaways 53
6.3 Recommendations 53

6.4 SUGGESTIONS FOR FURTHER RESEARCH 55

REFERENCES 56

APPENDIX A Participant information sheet 59

APPENDIX B Participant agreement form 61

APPENDIX C Instrument 63

LIST OF FIGURES

Figure 1: Effective Learning – Conceptual Framework

LIST OF ACRONYMS

CISM - Certified Information Security Manager

CISSP - Certified Information Security Professional

CEH - Certified Ethical Hacker

ESG - Enterprise Strategy Group

ISACA - Information Systems Audit and Control Association

ISC2 - International Information System Security Certification Consortium

ISSA - Information Systems Security Association

KSA - Knowledge Skills Abilities

CHAPTER 1. INTRODUCTION

1.1 Statement of purpose

This qualitative study investigates the potential role of online learning in addressing the prevalent shortage of cybersecurity skills within the South African financial services sector.

1.2 Background of the study

Organisations confront a myriad of business risks stemming from a deficiency in cybersecurity skills. These risks span from the exposure of confidential data due to cyber-attacks, to reputational damage resulting from public awareness of compromised organisational infrastructure, and financial losses associated with cyber-attacks. Research examining the impact of cyber-attacks on stock prices reveals that targeted firms endure losses ranging from 1% to 5% in the days following an attack. (Cashell et al., 2004)

A study examining the cybersecurity labour shortfall in Europe implies that organisations are susceptible to these risks due to a core issue: "The primary identified problem currently is the deficiency of cybersecurity skills amongst the workforce"(Blazic, 2021)

The scarcity of cybersecurity skills is a persistent issue that organisations worldwide must contend with. This problem permeates various industries and sectors on a global scale. The 2022 Fortinet study concerning the cybersecurity skills gap identified this as the foremost concern for leaders across all continents: 81% of leaders in France, 77% of leaders in North America, and 77% of leaders in Hong Kong expressed this concern. (Fortinet, 2022)

A study conducted by the International Information System Security Certification Consortium (ISC)² reveals that, despite the workforce gap having narrowed to 2.72 million (ISC2, 2021), the "absence of skilled/experienced cybersecurity personnel" remains the primary job concern among cybersecurity professionals. Furthermore, 65% of the participating organisations disclosed that they are experiencing a shortage of staff dedicated to cybersecurity.(ISC2, 2021)

Online learning is predominantly defined by authors as the access to educational experiences facilitated through the application of certain technologies (Moore et al., 2011) This denotes the delivery of learning content specifically designed to be disseminated using technology. Owing to the integration of technology, online learning enables readily accessible, digital, media-rich content (de Freitas et al., 2015), including graphical representations and video to convey its content.

Online learning is utilised in various contexts for the delivery of educational content. Notable applications include organisational compliance training where institutions employ a Learning Management System (LMS), a Course Management System (CMS), a Virtual Learning Environment (VLE), or even a Knowledge Management System (KMS) (Moore et al., 2011). Online learning proves particularly advantageous in such scenarios as it enables training on a broad scale. All employees can engage with and complete the content within a specified time frame. Another instance is university online courses, where technology is leveraged to deliver the curriculum to a larger student population. This latter example has gained increased popularity since the Covid-19 pandemic has necessitated limiting large gatherings of people in a single location. This predicament has prompted a global challenge to the education system and compelled educators to transition to online teaching methods(Dhawan, 2020)

The primary pedagogical differences associated with online learning enable the content to be:

- Customised and tailored according to the unique requirements of diverse students or professionals, online learning more effectively accommodates varied learner needs. (Zhu et al., 2020)

- More accessible and consumed by a broader audience. For instance, learning content from prestigious universities such as MIT and Harvard, which was previously available exclusively to a select group of students able to enrol at these institutions, is now accessible in an online format. This development essentially democratises access to education at all ages and stages (de Freitas et al., 2015)

Given the pedagogical distinctions of online learning, it becomes evident that its use facilitates the development of more flexible and enriched training content. Additionally, it fosters connectivity among more geographically dispersed communities of learners (de Freitas et al., 2015)

1.3 Research problem

The deficiency in cybersecurity skills implies that numerous organisations continue to grapple with filling positions within their respective cybersecurity functions. This study examines the potential avenues through which online learning might assist in mitigating the cybersecurity skills shortage within the South African financial services sector.

In the South African context, a significant contributing factor to the scarcity of cybersecurity skills is the limited provision of formal cybersecurity education at the university or college level. Formal education is defined as: "standardized and all learning institutions e.g., schools, colleges, universities, etc. comply with these standards" (ThroughEducation, 2019). Moreover, a desktop study of South African universities indicates the absence of dedicated honours and master's programmes in cybersecurity; however, a few short courses are available through certain universities, such as the University of Johannesburg (UJ), the University of the Western Cape (UWC), and the University of the Witwatersrand (Wits).

The limited provision of cybersecurity education at schools, colleges, and universities results in a low number of individuals being trained, as these institutions can only enrol a limited number of students for physical classes at any given time. In contrast, online learning courses are noted for their "ability to reach

large international audiences” (de Freitas et al., 2015), suggesting that greater numbers of individuals can be trained in cybersecurity skills through this medium.

The limitations of formal education lead professionals to acquire their skills either through on-the-job or hands-on experience or via cybersecurity certifications provided by specific vendors—training methods that come with their own set of restrictions. This viewpoint is supported by a joint study undertaken by the Enterprise Strategy Group (ESG) and the Information Systems Security Association (ISSA). In the study, the majority of the 489 participating cybersecurity professionals disclosed that they depend on "hands-on experience, basic certifications, and networking" for skills development (Oltsik & Lundell, 2021). Online learning can respond to the needs of professional learners(de Freitas et al., 2015), thus allowing organisations to tailor and adapt the learning experience to simulate the skills typically acquired in an on-the-job setting.

1.4 Research questions

The study aims to address the following research questions through a comprehensive analysis of the literature, complemented by empirical data gathered via interviews with cybersecurity professionals:

1. What format of learning do cybersecurity professionals prefer?
2. What are some of the strengths and weaknesses of online learning in the cybersecurity domain?
3. Is online learning effective at teaching critical cybersecurity skills?

1.5 Rationale

Organisations are confronted with numerous business risks stemming from a deficiency in cybersecurity skills. Such risks range from the exposure of confidential data due to cyber-attacks and financial losses associated with these attacks, to reputational damage arising from public awareness of compromised organisational infrastructure. A study examining the cybersecurity labour shortfall in Europe implies that organisations are susceptible to these risks owing to a core

issue: "The primary identified problem currently is the deficiency of cybersecurity skills amongst the workforce"(Blazic, 2021)

This study intends to explore the various formats through which cybersecurity skills can be acquired, with a particular emphasis on online learning. The proposed questions aim to elucidate the following critical aspects:

- Whether online learning is a preferred method of learning for cybersecurity professionals, or if they favour other methods or formats, and
- How effective, in their experience, online learning is for enhancing the skills of cybersecurity professionals.

The findings of the study may offer valuable insights to cybersecurity professionals involved in any capacity of the recruitment process. This includes organisational leaders seeking to fill roles within their respective organisations, as well as cybersecurity professionals searching for effective means to acquire skills.

1.6 Delimitations of study

The primary data for this study is sourced from the South African financial services sector. The evaluation of different training methods is confined to the following formats or types:

- **On-the-job training**: Skills obtained through hands-on experience
- **Formal learning**: NQF level studies based on the National Qualifications Framework.
- **Certifications:** Cybersecurity certification obtained through cybersecurity vendors, e.g., CISSP, CISM, and ISACA certifications.
- **Online learning:** the access to educational experiences facilitated through the application of certain technologies

The study targets a population confined to the South African financial services industry. Any additional sectors and training formats fall beyond the purview of this study.

1.7 Definition of terms

Capture The Flag (CTF): Small teams of participants exercise their cybersecurity skills by solving various tasks in an online learning environment. (Švábenský et al., 2020)

Certification: Proof or a document proving that someone is qualified for a particular job or that something is of good quality. (Thesaurus)

Cyber training labs: A popular form of cybersecurity education, where students solve hands-on tasks in an informal, game-like setting (Švábenský et al., 2020)

1.8 Assumptions

- The research participants will respond to all the questions sincerely and candidly.
- The research participants are well-acquainted with the cybersecurity terms used, as they are integral to their roles (SkillSoft)
- The theoretical basis of the study is precise.
- The findings of this study will apply to all cybersecurity training within a South African financial services context.

CHAPTER 2. LITERATURE REVIEW AND THEORETICAL FRAMEWORK

2.1 Introduction

A plethora of literature has been published concerning the worldwide cybersecurity skills gap. The bulk of these publications delve into global statistics regarding the skills shortage, cybersecurity competencies presently in high demand by organizations, and, occasionally, discourses on necessary measures to mitigate this skills deficit. This study aims to provide an additional viewpoint on how to address the skills shortage, primarily concentrating on the potential benefits of online learning.

Many published works offer a global viewpoint, often articulating perspectives from the United States or Europe. In contrast, this study will seek to correlate these perspectives with a South African context, particularly within the financial sector.

The literature review will be structured thematically, centred around the following key themes discerned throughout the literature:

- Upskilling & Training Resources
- Different Formats of Acquiring Cybersecurity Skills
- Key Considerations of Online Learning
- The Overall Effectiveness of Online Learning

2.2 Definition of topic or background discussion

Consistent evidence in the literature suggests that the resolution to this issue lies in upskilling and training resources. A view illustrated in a 2019 study by ISC2 proposes that "by aiding in the training and development of existing team members, organizations can enhance their security posture and help bridge the gap in their respective corners of the world" (ISC2, 2019). This perspective is echoed in a study by (McGettrick et al.)which implies that the "talent deficit has

precipitated a demand for increased and improved cybersecurity training". (McGettrick et al.) Finally, a study by the European Union Agency for Cybersecurity indicates that "defenders have elevated their training levels to offset the skill shortage in the area of cyber threat intelligence" (Cybersecurity, 2019)

With this understanding of what is needed to address the issue, the next selection of publications to be examined revolves around the various formats through which cybersecurity skills can be acquired.

The literature reveals that each different format possesses its strengths and weaknesses, of which organizations must be cognizant. A study by Steven Furnell proposes that "the diversity of the cybersecurity domain may complicate the task of identifying qualifications or certifications that can serve as indicators of the skills relevant to a specific situation" (Furnell, 2020). This viewpoint is mirrored in a study recommending that a clear understanding of the varying needs of cybersecurity training "should guide the design of the curriculum for cybersecurity educational programs" (Blazic, 2021)

In the context of this investigation, the specific learning styles for cybersecurity training, as found in existing literature, are as follows:

- **On-the-job training (physical):** This term refers to the acquisition of skills through the daily tasks of a specific role. It is also perceived as formally structured activities such as apprenticeships and other training programs. (Mincer, 1962)
- **Classroom-style training:** This is a physical learning environment where pupils acquire knowledge and instructions from an educator. It represents a prevalent teaching style where an instructor, positioned in front of approximately 20–25 students, imparts information. (Shuell, 2001)
- **Online learning:** This type of training is delivered through the medium of technology, allowing access to learning experiences. (Moore et al., 2011). Learning that offers learners the opportunity to participate in courses and programs from remote locations with the help of Internet technology. (Kamble et al., 2021)

- **Online self-paced training:** This approach, a subset of online learning, provides more autonomy to learners. It enables each learner to advance at a personalized pace, simultaneously offering benchmarks for tracking progress and achievement. (Rhode, 2009)
- **Online instructor-led training**: This category of online learning involves a live instructor who conveys training to a group of learners utilizing video conferencing software or other online tools.

The subsequent consideration acknowledges that individuals may exhibit different preferences for learning styles. Learning styles are defined as the "characteristic cognitive, affective, and psychosocial behaviours that serve as relatively stable indicators of how learners perceive, interact with, and respond to the learning environment" (Cook & Smith, 2006). This observation suggests that cybersecurity professionals might favour different learning formats. And as stated by (Collins, 1982) students have differing access to comprehension practice. Therefore, it is crucial to ascertain the learning format that cybersecurity professionals prefer. This leads to the research question: Which learning format do cybersecurity professionals prefer? Do they favour on-the-job training, classroom-style training, or online learning?

Each of these training formats possesses inherent strengths and limitations. Both on-the-job training and classroom-style training have extensively documented details regarding their respective advantages and disadvantages. In contrast, concerning online learning, what is conspicuously obvious and inadequately addressed are the elements of online learning's strengths and limitations, as well as the components organizations need to concentrate on to harness this learning format's full potential. This observation indicates the importance of investigating this area, leading to the subsequent research question: What are the key considerations of online learning? And, upon considering these aspects, would online learning be pertinent to the cybersecurity domain?

Finally, is there sufficient empirical evidence to assert that online learning is an effective training format? This leads to the final research question: Is online learning efficacious in teaching crucial cybersecurity skills?

2.3 What format of learning do cybersecurity professionals prefer?

The core concepts surrounding the different formats primarily revolve around the method by which a cybersecurity professional is trained or upskilled in a particular cybersecurity skill.

2.3.1 *On-the-job training*

The findings from the literature review indicate that this training format is among the more dominant methods employed. This perspective is evident in a study by (Keith S. Jones et al., 2018), wherein the study's findings demonstrated that, on average, "56.02% of participants responded that they had learned the most about any given KSA at work." Additionally, a study by ESG reveals that "52% of the respondents suggested that hands-on training is the most important" (Oltsik & Lundell, 2021)

The challenge with this training method is that numerous organizations require proficient individuals and do not have the luxury of training resources. The majority of organizations demand "relevant and extensive work experience, advanced knowledge of concepts, and cybersecurity certifications" (ISC2, 2019)

Furthermore, organizations have a limited number of resources that they can hire and provide with on-the-job training. The resultant number of trained individuals proves insufficient to significantly address the current shortage in cybersecurity skills.

2.3.2 *Classroom-style training*

The findings from the literature review suggest that this is among the more favoured formats for learning cybersecurity skills, as many accredited vendors offer classroom-style training for popular certifications. This format enjoys popularity due to the wide array of certifications from which to choose. A study by (Oltsik & Lundell, 2021) lists the top five certifications recommended by respondents: Certified Information Systems Security Professional (CISSP),

chosen by 51% of the respondents; Certified Information Security Manager (CISM), chosen by 25%; CompTIA Security+, selected by 24%; Certified Information Security Auditor (CISA), selected by 19%; and lastly, Certified Ethical Hacker (CEH), chosen by 17% of the respondents. In South Africa, two notable accredited vendors, CompTIA and Torque-IT, offer classroom-style training for these certifications. CompTIA purports to provide best-in-class instructor-led training for both individuals and teams (CompTIA).

2.3.3 *Online learning*

The findings from the literature review suggest that this format offers several features making it easily accessible to all cybersecurity professionals and adaptable to specific organizational needs. Online learning enables us to "find new ways to fit learning into our lives and, capitalizing on the open access paradigm, connect non-co-located communities of learners through online learning content delivery and mobile access" (de Freitas et al., 2015). This evidence demonstrates the format's flexibility and its ability to be tailored according to specific requirements. This study will focus on the following two subsets of this format:

- **Online self-paced training (SPT)** - Online self-paced training denotes an instructional design approach permitting learners to access and engage with learning materials according to their own preferred time, place, and pace. This training mode provides learners the flexibility to control the speed and sequence of their learning, thereby enabling them to personalize their learning experience to meet their individual needs and preferences. (Garrison & Vaughan, 2008)
- **Online instructor-led training (ILT)** - Online instructor-led training involves a facilitator leading the training session virtually, using various communication tools and multimedia resources to engage learners and foster meaningful interactions. The instructor guides the participants through the course material, provides explanations, facilitates discussions, and addresses questions or concerns in real-time, creating an immersive and collaborative learning environment. (Jung, 2019)

2.3.4 *Proposition 1*

According to the literature, online learning appears to be the most suitable for cybersecurity training due to its format. Professionals can access online training from anywhere globally, and the training can be customized to cater to specific cybersecurity skills, whether technical or non-technical.

2.4 What are some of the key considerations for online learning?

The following list of key considerations has been identified when formulating an online training curriculum for upskilling cybersecurity professionals.

2.4.1 *Quality, Low Retention, Need for Engagement*

A study by (de Freitas et al., 2015) suggests that the following key determinants should be considered as part of an online learning curriculum:

- Quality: This term refers to the content quality contained in the training material.
- Low retention: This is linked to the quality issue. If the online training is not of high quality, it will result in low retention and ultimately low training completion.
- The need for engagement: The study indicates that students need to interact with fellow students in the same field to exchange ideas and recommendations.

2.4.2 *Proposition 2*

If training content providers ensure that aspects of self-efficacy, quality, low retention, and the need for engagement are addressed, online learning can become a highly effective method for training cybersecurity skills.

2.5 Is Online learning effective at teaching critical cybersecurity skills?

With all aspects considered, what does the data analysis indicate regarding the overall effectiveness of online training? More detailed information will be obtained from the data analysis to answer this question.

2.5.1 *Proposition 3*

All factors considered, the findings suggest that if online training content is created to be more engaging, higher quality, and maintains high retention, it will be the most effective form of cybersecurity training.

2.6 ANALYTICAL FRAMEWORK

2.6.1 *Theoretical Framework*

Bandura's social learning theory, widely used to understand how people learn through observation, imitation, and modelling, is applied in this paper. Bandura's four principles of attention, retention, reproduction, and motivation are used to analyse the strengths and weaknesses of online learning.

The key constructs and variables associated with online learning are analysed using Bandura's Social Learning Theory. This theory "takes into account a person's past experiences, which factor into whether behavioural action will occur" (LaMorte, 2019). The four key constructs part of the social learning theory include attention, retention, reproduction, and motivation (Refer to Figure 1: Effective Online Learning – Conceptual Framework)

- Attention: This construct focuses on the learning content's ability to capture the learner's attention. The Social Learning Theory suggests that "if the model is attractive, prestigious, or appears particularly competent, you will pay more attention" (Nickerson, 2022). The individual needs to pay attention to the behaviour and its consequences and form a mental representation of the behaviour. (McLeod, 2011)

- Retention: This construct underlines the importance of learners retaining the content they have learned. How can the cybersecurity content be retained in a way that allows the professional to gain new skills and competencies? Retention is vital because low retention rates negatively impact lost tuition, non-completion's emotional effect, and graduation delays(Ali & Leeds, 2009)
- Reproduction: This construct, directly correlated to the attention and retention constructs, focuses on the learner's ability to reproduce the skills and competencies acquired through these constructs.
- Motivation: The final construct emphasizes the learner's motivation to continue with the tasks at hand. In this study's context, what motivation does the cybersecurity professional have to complete this learning content?

2.6.2 *Conceptual Framework*

To address the deficiency of cybersecurity resources in the South African Financial Services sector, it has been identified that training and upskilling IT professionals who are entering the cybersecurity field, or cybersecurity professionals aiming to enhance their skills, are the recommended steps. The most accessible training method is online learning. To ensure the effectiveness of this method, the following key constructs for effective learning have been recognized: Attention, Retention, Reproduction, and Motivation.

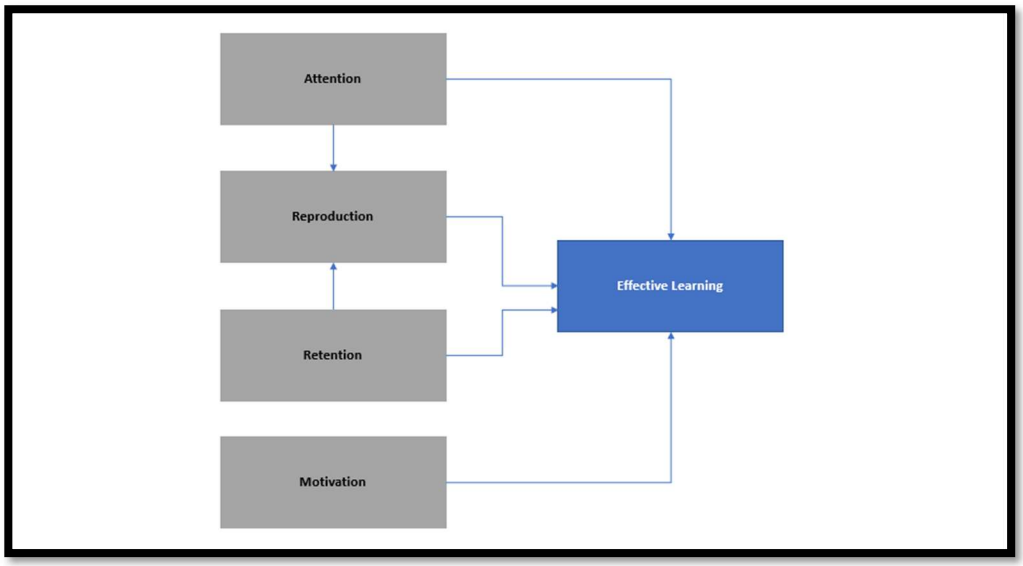


Figure 1: Effective Learning – Conceptual Framework

In conclusion, the solution to the lack of cybersecurity resources involves upskilling and training. Different training formats possess inherent strengths and shortcomings, which need thorough consideration to address a problem of such magnitude. Online Training showcases several strengths, and online delivery of ICT programs is experiencing rapid growth, (Myers et al., 2014) making it an ideal candidate for the preferred training format. This study aims to determine its relevance for upskilling individuals in the cybersecurity domain.

2.6.3 *Proposition 1*

Based on the literature, online learning appears most suited for cybersecurity training due to its flexible format. Professionals can access online training globally, and the training can be tailored to meet specific cybersecurity skills requirements, whether technical or non-technical.

2.6.4 *Proposition 2*

Assuming that training content providers address aspects of quality, low retention, as well as the need for engagement, online learning could become an exceedingly effective method for training cybersecurity skills

2.6.5 *Proposition 3*

In light of all considerations, the findings suggest that online training content that is engaging, high-quality, and maintains high retention could prove to be the most effective form of cybersecurity training.

CHAPTER 3. RESEARCH METHODOLOGY

3.1 Research approach

Upon reviewing the literature, it was discovered that each training format has its own set of advantages and drawbacks. To delve deeper into the personal experiences of various cybersecurity professionals, a qualitative research methodology was employed. The selection of this research methodology was influenced by a multitude of factors, among them the research questions, the type of data required to answer these questions, and the theoretical framework. According to (J. W. Creswell, 2014), the qualitative research approach "entails emerging questions and procedures, data collection typically taking place in the participant's setting, data analysis inductively building from particulars to general themes, and the researcher making interpretations of the data's meaning." The qualitative research approach facilitated the gathering of contextual information about the experiences of cybersecurity professionals within their specific fields.

Employing a qualitative approach is optimal for generating a thorough understanding of a professional's learning experiences within a specific cybersecurity domain, their encounters with various training formats, and their impressions of the learning process's efficacy. The use of a qualitative approach enabled the collection of rich, detailed data that was subsequently analysed to gain a deeper insight into the experiences of cybersecurity professionals.

Having reviewed multiple studies to comprehend key theories and factors that can influence online learning effectiveness, this study examines whether these theories and factors apply to cybersecurity professionals in the South African financial services industry. This method posits that the efficacy of online learning may differ based on the factors that various cybersecurity professionals deem influential.

3.2 Research design

The decision to employ a cross-sectional research design in this study was primarily driven by the research questions that the study intended to answer, as the research question determines the most suitable study design. (Johnson, 2010)

A cross-sectional research design is a type of methodology in which data is gathered from a group of individuals or organisations at a single moment in time. There are several advantages to this design that justify its application in this study:

1. **Speedy data collection**: A cross-sectional study design involves data collection at a single point in time (Johnson, 2010), making it highly appropriate for this study given the time restrictions and the availability of cybersecurity professionals to supply the necessary data to address the research question.

2. **Broad scope:** A cross-sectional research design permits a wide research scope, as it can encompass many participants and cover an extensive range of variables or issues. The cybersecurity field is made up of various sub-domains, each possessing unique factors that demand meticulous consideration. Cybersecurity presents a complex challenge that necessitates interdisciplinary reasoning (Craigen et al., 2014)

3. **Simplicity in analysis:** Cross-sectional research designs simplify analysis as the data is collected at a single moment in time, thereby eliminating the need for complex statistical analyses.

4. **Suitability for exploratory research:** Cross-sectional research design proves valuable for exploratory research, where the researcher intends to collect data to generate hypotheses and suggestions for future research directions. (Johnson, 2010)

3.3 Data collection methods

The data collection method for this study involved conducting semi-structured interviews with participants, facilitated through Microsoft Teams. Comprehensive information about the study's objectives was provided to potential participants, granting them ample time to consider their participation. The final sample for the study included ten participants who had consented to participate.

The interviews utilized open-ended questions to inspire participants to offer in-depth details concerning their experiences. Microsoft Teams offered a built-in function to record and transcribe the interviews. However, to ensure the accuracy of the transcriptions, they were compared to the original audio to correct any potential discrepancies arising from the transcription process.

The research instrument consisted of a series of questions that were grouped according to the research question they were designed to address. Individual interviews were conducted to glean a detailed understanding of each respondent's personal experience.

3.4 Population and sample

3.4.1 *Population*

The population targeted for this study comprised cybersecurity professionals employed in the South African financial services sector. These professionals, being domain experts in cybersecurity and its associated training, shared feedback related to the following research questions:

1. What learning format do cybersecurity professionals prefer?
2. What are the strengths and weaknesses of online learning in the cybersecurity domain?

Subsequently, feedback was sought from senior or management-level cybersecurity professionals on the following question:

3. Is online learning effective at imparting crucial cybersecurity skills?

Management-level professionals were chosen for this feedback due to their ability to provide a professional perspective on the skills and competencies of their staff members, both before and following online training.

To ensure a diverse range of expertise within the cybersecurity domain, the selected population included individuals with varying specialisations, from technical roles such as security operations centre analysts and penetration testers to non-technical roles related to policy development and implementation. This approach ensured data was collected from respondents necessitating a combination of both technical and non-technical skills in the cybersecurity field.

For this study, the researcher reached out to 28 potential participants from the target population, with 10 eventually participating in the study.

3.4.2 *Sample*

The selection of the ten cybersecurity professionals involved a combination of snowball and purposive sampling methods, a decision necessitated by the limited availability of cybersecurity professionals. Purposive sampling was implemented to identify respondents capable of providing pertinent responses to the research questions. Moreover, the snowball sampling method was adopted to augment the sample size, which involved asking existing cybersecurity participants to recommend other individuals who could contribute valuable insights relevant to the research question.

3.5 The research instruments

The interview comprised 16 open-ended questions, divided into four sections: demographics, format, strengths and weaknesses, and effectiveness. These sections can be found in Appendix D.

The interview questions were organised into three sets. The first set prompted respondents to specify their preferred format of cybersecurity training. The second set focused on the critical factors essential for successful online learning.

The final set solicited the respondents' views on the efficacy of online learning in imparting cybersecurity skills within their respective areas of specialization.

Before commencing each session, the respondents were briefed on the structure and strategy of the interview. Additionally, the problem statement and research question derived from the study were clearly articulated to the participants, underlining the study's objectives.

3.6 Data Collection

The particulars of the study were provided to each potential respondent. Those expressing interest in participation signified their consent to engage in the study by responding. Invitations to Microsoft Teams meetings were sent to these respondents for discussing the research questions and obtaining their feedback.

Interview sessions, totalling ten, were held between December 18th, 2022, and January 15th, 2023. Each session spanned an average of 30 minutes. Conducted online, these interviews were recorded using MS Teams and were subsequently transcribed

3.7 Data analysis strategies and interpretation

Data analysis was conducted via Thematic Content Analysis (TCA). This process involved organizing the data, undertaking a preliminary read-through of the database, coding and organizing themes, representing the data, and forming an interpretation of them (J. Creswell, 2013). The procedure was as follows:

Data collected from the interviews was organized according to the different respondents and the specific similarities they shared. This organization facilitated the identification of common themes that articulated the shared perspectives among participants (Anderson, 2007). These themes were structured and presented in an organized manner, and the data was then interpreted, with the findings subsequently shared in detail.

3.8 Quality Assurance

3.8.1 *Transferability*

Transferability is attained when readers discern that the research narrative aligns with their situation, enabling them to intuitively apply the research findings to their circumstances (Tracy, 2010)

This study endeavours to ensure transferability by presenting information obtained directly from cybersecurity professionals who experience the cybersecurity skills shortage daily (hiring managers), as well as those who have experienced multiple training formats and identified the format most effective for their specific specialization.

The outcomes of this study will be conveyed to other individuals in the South African Financial Services sector, who will then be equipped to apply the study's findings. As such, the results of this research apply to individuals in the South African Financial Services sector, who can utilize the findings to inform their actions and decisions.

3.8.2 *Credibility*

Credibility pertains to the trustworthiness, verisimilitude, and plausibility of the research findings (Tracy, 2010). This study will ensure credibility in the following ways:

- The individuals who participated in the research possess considerable experience in the cybersecurity domain and can be regarded as reliable sources.
- The researcher, holding tacit knowledge of the study's themes and constructs and possessing extensive experience in the cybersecurity field, has a first-hand understanding of the implicit, assumed issues that have become a common understanding among the participants.

- A thorough collection of respondents' real-life experiences will be accumulated and cross-referenced with feedback received from other participants, thereby ensuring a "thick description" (Tracy, 2010).

3.8.3 *Dependability*

Dependability refers to the consistency and reliability of the research findings and the extent to which research procedures are documented, enabling an external party to follow, audit, and critique the research process (Sandelowski, 1986)

To ensure dependability, this study adopted a systematic approach to collect, organize, and present the data. The researcher diligently adhered to a structured and methodical process in determining the target population, conducting interviews, logging responses, and managing other relevant aspects of the study.

3.9 Ethical considerations

This study conformed to ethical guidelines as stipulated by the University of the Witwatersrand. The initiation of the study only proceeded after approval was obtained from the University's ethics committee, as outlined in Appendix E. The study followed the subsequent ethical considerations:

- No participant was subjected to any form of risk or harm while partaking in the research.
- The study's details and objectives were communicated to potential participants.
- Written consent was acquired from each participant before the initiation of the study.
- The confidentiality and anonymity of the participants were rigorously maintained.

CHAPTER 4. PRESENTATION OF DATA

4.1 Data Collection

4.1.1 *Introduction*

In this chapter, the data gathered by employing the methods and techniques detailed in Chapter 3's research methodology section are presented. Three research questions were formulated and addressed via a comprehensive literature analysis and empirical data procured from interviews conducted with cybersecurity professionals.

Ten respondents, selected based on their expertise in the cybersecurity domain, were included in this study. As professionals in cybersecurity, these participants provided insight into several aspects pertinent to cybersecurity training. Specifically, they conveyed their preferences for learning formats, pinpointed the strengths and shortcomings of online learning within the cybersecurity domain, and evaluated the efficacy of online learning in imparting vital cybersecurity skills.

The results of this study are delivered in a narrative style, encapsulating the dialogues and feedback received from the participants. The feedback obtained has been arranged according to the research question and the research instrument questions that are correspondingly mapped to each research question.

4.1.2 *Research Question 1*

This section conveys a spectrum of data, including the tenure of each respondent within the cyber domain; their specific roles in cyber operations; their perception of their roles as technical or non-technical; the number of cyber training programs attended; the variety of formats in which the training was delivered; their preferred training format and the reasons behind such preference. This information offers critical context and background about the participants, thereby enhancing the comprehension of their feedback and responses to the research questions.

Experience and Roles of the Respondents

Participants displayed diverse years of experience in the cybersecurity domain, ranging from a span of two years to 13 years. The roles they held and the organisations they served varied over time, including positions like IT analyst, identity and access management analyst, and cybersecurity consultant, thereby indicating a broad spectrum of experience and exposure across different cybersecurity areas.

Six participants primarily carried out roles and responsibilities focused on operational day-to-day activities, while the responsibilities of four participants were more aligned with the strategic or managerial objectives of their organisations.

Two participants classified their roles as exclusively technical, whereas eight participants stated their roles encompassed both technical and non-technical aspects. None of the participants classified their roles as solely non-technical.

The participants reported attending a range of four to ten training programs, delivered in diverse formats such as on-the-job training, online training, and traditional in-person instructor-led training.

Format of Training

All participants confirmed that they had undergone training in different formats, including on-the-job training. Eight of them reported receiving online training, while two mentioned participating in traditional, physical classroom-style training.

Six participants expressed a preference for online, self-paced training, attributing their preference to its inherent flexibility. This adaptability enables them to schedule their training around their demanding timetables. Respondent 6 particularly highlighted that this training format allows individuals to progress at their speed, revisit any sections they may have overlooked, or bypass topics with which they are already familiar.

4.1.3 *Research Question 2*

This section elucidates the online learning preferences of cybersecurity professionals, spotlighting their favoured aspects and grievances concerning various elements of online learning. Furthermore, it elucidates the crucial components necessary for online learning within the respondents' specific cybersecurity sub-domain and concludes with an examination of the strengths and weaknesses of cybersecurity training, as perceived by the respondents.

Cyber training completed

Six participants appreciated the most the capacity to complete their training at their own pace and convenience. Respondent 5 accentuated that self-paced training facilitated enhanced value extraction and proved particularly beneficial amidst their intense workload.

Four participants underscored the multimedia composition of the training content, encompassing video, audio, and graphics, as one of the aspects they appreciated the most. Respondent 6 articulated that multimedia aids in faster knowledge assimilation when the course is informative and well-structured.

In terms of what they least enjoyed about the training, diverse answers were received, although some responses demonstrated similarities among the participants.

Five participants expressed their aversion to content that failed to engage them and lost their interest. For instance, Respondent 5 pointed out that pre-recorded sessions are monotonous and unproductive, as they merely involve observing someone speaking without any interaction. Six participants also identified the lack of collaboration or interaction with fellow students in online, self-paced training as a significant disadvantage. Respondent 8 underscored the necessity for having the option to seek further information or clarification when needed.

Key considerations

When participants were probed about the key aspects to consider concerning online training in their distinct cybersecurity sub-domains, the responses varied based on their areas of expertise. Given that they hail from different cybersecurity sub-domains, their answers varied in terms of depth and focus.

Two participants highlighted the importance of initiating with basic cybersecurity skills pertinent to their specific sub-domain. For example, Respondent 8 expressed that training programs must commence with fundamental security aspects, such as email security.

Five participants underscored the necessity of segmenting extensive training content into smaller, more manageable parts to enhance engagement and comprehension. Respondent 4, for instance, explained that dissecting content into smaller portions would sustain learner engagement and facilitate better information absorption.

Strengths of online training

When queried about the strengths and weaknesses of online training in their distinct sub-domains, all respondents offered feedback indicating that online learning offers a more cost-effective alternative. Two respondents explicitly pointed out that online training eradicates the requirement to commute to a specific location for training, leading to considerable cost savings. Respondent 5 also emphasised the cost-effectiveness of online training, as it enables learners to access the training from any location, eliminating the need for travel.

Three participants observed that online training results in cost savings for training providers, as they are relieved from catering food and refreshments for the attendees. This reduction in the overall cost of the training program can be transferred to the learners either through reduced fees or increased investment in course development.

Five respondents underscored that online training content can be more engaging than traditional learning methods, such as reading from a book or attending a lecture. This is attributed to the integration of creative and engaging multimedia elements, including videos and music, into the learning content.

Weaknesses of online training

The responses concerning the weaknesses of online training differed due to the varying sub-domains of the respondents within the cybersecurity domain. One respondent observed that online training is confined to teaching basic skills and might not be effective in cultivating the advanced skills necessary for higher-level roles. Another respondent identified a drawback of online learning as the difficulty in comprehending content delivered by instructors with unfamiliar accents. Respondent 2 acknowledged their occasional struggle in understanding instructors with unfamiliar accents, requiring them to concentrate more on understanding the material.

Similar responses were noted among several respondents regarding the weaknesses of online training. Three respondents highlighted the lack of collaboration when learning from self-paced online content. They expressed that the absence of an instructor, to whom immediate queries can be directed, is a significant disadvantage. Respondent 4 asserted that collaboration is crucial for effective learning and is currently missing in online training.

4.1.4 *Research Question 3*

This section elucidates the respondents' views on the appropriateness of online learning for delivering both technical and non-technical training. Additionally, it explores their thoughts on the effectiveness metrics that can be applied to cybersecurity training within their particular subfield. The respondents were also

queried about their opinions on the efficacy of online training for developing skills in their specific cybersecurity specialisation.

Technical and Non-technical elements

When questioned about the efficacy of teaching technical skills online, all respondents concurred that certain technical components can be effectively imparted through online training. Respondent 1 proposed that individuals could gain access to a virtual environment where they can perform practical labs. In contrast, Respondent 2 revealed their personal experience of acquiring technical skills through online process documentation.

Regarding the effectiveness of training non-technical skills online, two respondents expressed slight reservations. Respondent 8 suggested that while possible, face-to-face interaction might be more conducive for honing soft skills. Respondent 7 noted that effective online non-technical training would necessitate a blend of resources, including instructor assistance and supplemental materials used in conjunction. Nonetheless, eight respondents agreed that non-technical training components could be efficiently delivered through online mediums.

When prompted to offer perspectives on measures of effectiveness for online training within their specific cybersecurity sub-domain, a range of responses was obtained. However, a primary response, common among all respondents, was the importance of practically applying the knowledge acquired during the training. The respondents maintained that training effectiveness is best manifested when the skills gained can be utilised in day-to-day operational and strategic activities, thereby adding value to the organisation.

When asked if online training is effective in cultivating skills within their respective cybersecurity sub-domains, all respondents unanimously agreed that it represents an effective methodology.

CHAPTER 5. ANALYSIS & FINDINGS

5.1 Introduction

This chapter presents an analysis of the primary outcomes derived from the research. The research examines the training format preferences of cybersecurity professionals within the South African financial services industry. The evaluation of these findings is provided herein, highlighting key trends and patterns that emerged from the study.

Chapter 2 of this research study incorporates the Literature Review and Theoretical Framework. In this chapter, key elements of Bandura's Social Learning Theory are identified and explored in detail (please refer to Table 1: Four Principles of Bandura's Social Learning Theory). These components, combined with the feedback received from each participant, are deemed contributing factors to the analysis conducted in this study. The main objective is to investigate the relevance of the constructs derived from the literature review and theoretical framework, specifically for cybersecurity professionals and their learning preferences.

Attention	**Retention**	**Reproduction**	**Motivation**
Ability to pay attention to the learning material	Ability to remember the observed behaviour	Ability to replicate the learned material	Motivation to learn the material

Table 1 Four Principles of Bandura's social learning theory

5.2 Bandura’s Social Learning Construct – Attention

This construct emphasises the necessity for the learning content to capture the learner's attention effectively. As suggested by the Social Learning Theory, "if the model is appealing, prestigious, or seems exceptionally competent, more attention will be paid" (Nickerson, 2022)

5.2.1 *Which learning format do cybersecurity professionals prefer?*

The study incorporated the following training formats: physical on-the-job training, physical classroom training, and online training.

The attention principle underscores the importance of focusing on environmental stimuli for acquiring new knowledge and skills. Such interactions allow for the construction of knowledge in a meaningful and memorable manner. (Rhode, 2009) Moreover, this principle suggests that those who pay more attention to a particular training format are more likely to retain the learned information.

The study's findings revealed that all ten participants demonstrated attentiveness to their received training, regardless of the delivery format. However, the amount of attention devoted to each format differed among individuals, reflecting their personal preferences for various training formats. This suggests that some formats might be more successful in capturing attention than others. This view aligns with (Rhode, 2009) who posits that, depending on specific circumstances, not all forms of interaction may be valued equally by learners or be as effective.

Feedback from participants indicated a desire to further divide online training into two subcategories: online self-paced training and online instructor-led training, owing to the distinct strengths and weaknesses each format presents in holding the learners' attention.

Six participants expressed a preference for online self-paced training due to its flexibility, allowing learners to accommodate their training around their busy schedules. This preference could be attributed to this training format's ability to captivate the learner's attention, enabling them to engage with the material at their own pace and on their terms.

Similarly, physical classroom-style training was favoured by two participants as it facilitated real-time interaction with trainers and peers, thus promoting their attention and engagement. These findings align with (Collins, 1982), who argues that the quality of conversational exchanges between teachers and students influences student achievement.

On-the-job training, which allowed participants to learn in real-time with hands-on experience and immediate knowledge application, was reported to be particularly beneficial for those in operational roles.

Physical classroom training, involving in-person classes or workshops, allowed for direct interaction with instructors and fellow participants. Participants who underwent this type of training reported that it provided a more structured learning experience, along with the ability to focus on the material presented. This format was preferred due to the physical presence of an instructor, a finding supported by (Kamble et al., 2021), who argue that the physical absence of an instructor significantly impacts the learners.

Online training was popular among participants, with eight reporting experiences with this format, either as online instructor-led training or online self-paced training. Participants cited the flexibility of online training as a key factor in its popularity, allowing them to accommodate their training around their work and personal commitments.

In conclusion, the attention principle plays a critical role in cybersecurity training. The study's findings suggest that training formats capturing individuals' attention may facilitate learning and retention more effectively. Therefore, training programs should be designed to cater to participants' attentional preferences, with further research potentially exploring the relationship between attention and retention across various cybersecurity training formats.

5.2.2 *What are the strengths and weaknesses of online learning?*

Online learning offers cybersecurity professionals the flexibility to harmonize their work and learning schedules. This format, referred to as "new learning" or more flexible learning by (de Freitas et al., 2015), enables cybersecurity professionals to learn at their own pace. The convenience potentially mitigates the stress associated with traditional classroom learning, which demands adherence to a fixed schedule. Moreover, online learning platforms offer a multitude of resources and tools capable of enriching the learning experience, including interactive simulations, virtual labs, and multimedia content. Such multimedia content, through interactive digital elements, can render learning more engaging (de Freitas et al., 2015)

The absence of physical interaction with instructors and peers may generate a sense of isolation and disconnection, possibly leading to a reduced sense of community and engagement. Additionally, without the advantage of real-time feedback and support, learners may struggle to maintain motivation and focus, negatively impacting learning outcomes. This perspective is supported by (Kamble et al., 2021) who underscore the significance of interactions between learners and instructors.

Furthermore, the online environment can introduce new distractions that hinder learning. Cybersecurity professionals may be tempted to check their email, social media, or other online platforms during the learning process, resulting in diminished attention and focus. This issue of distractions is underscored by (Kamble et al., 2021) who mentioned the learners' inability to concentrate during the sessions due to various distractions.

5.2.3 *Is Online learning effective at teaching cybersecurity skills?*

The data indicate that online training can effectively impart technical skills by offering a virtual environment conducive to conducting practical labs, which can be highly engaging and interactive.

Nonetheless, some respondents expressed reservations regarding the effectiveness of online training for non-technical skills, such as soft skills. They suggested that face-to-face interaction might be more conducive to developing these skills, given its provision for more personal and direct engagement with instructors and peers. (Myers et al., 2014) underscore the importance of developing soft skills in the cybersecurity field, stating that professionals should possess effective interpersonal and communication skills. This indicates that maintaining attention could prove more challenging for non-technical training delivered online, with face-to-face interaction potentially being more engaging in this context.

However, it's worth noting that online learning platforms can still employ strategies to enhance attention and engagement for non-technical training. For instance, interactive multimedia content, group discussions, and collaborative projects can all serve as effective tools for keeping learners engaged and focused on the material. Additionally, equipping learners with clear and specific learning objectives can bolster their motivation and focus.

In summary, the data suggest that attention is a crucial consideration in the context of online learning for cybersecurity professionals. Strategies should be implemented to foster engagement and maintain focus, particularly for non-technical training. By incorporating an array of interactive and engaging tools and strategies, online learning platforms can facilitate learners' development of both technical and soft skills, while also nurturing a sense of engagement and motivation.

5.3 Bandura's Social Learning Construct – Retention

This construct underscores the significance of a learner's ability to retain the content they have assimilated. The paramount concern is the depth to which the behaviour has been committed to memory. While the behaviour might be observed, it is not consistently remembered, thereby thwarting imitation. Thus, it becomes critical to form a memory of the behaviour for future replication by the observer. (McLeod, 2011) The pertinent question that arises is: how can cybersecurity content be retained in such a manner as to enable professionals to acquire new skills and competencies?

5.3.1 *Which learning format do cybersecurity professionals prefer?*

The principle of retention pertains to the capacity to store and retrieve information garnered from learning experiences. Retention in online education poses a significant concern for students, faculty, and administration alike (Ali & Leeds, 2009). Within the scope of cybersecurity training, the capability to retain knowledge and skills becomes essential for professionals to implement them proficiently in their everyday responsibilities.

The capability to retain knowledge and skills is additionally dependent on the frequency of training. The study revealed that participants attended numerous training programmes throughout their careers, underscoring the necessity for continuous training to remain current with the field's latest progress and advancements.

In conclusion, the principle of retention underscores the necessity for well-designed training programmes aiming to foster long-term retention of knowledge and skills. Regarding cybersecurity, this becomes imperative for professionals to stay abreast with the rapidly evolving threat landscape and to effectively safeguard their organisations.

5.3.2 *What are the strengths and weaknesses of online learning?*

The analysis indicates that online learning bestows cybersecurity professionals the advantage of revisiting and reviewing course materials multiple times, thereby facilitating information retention. Learners can return to and review complex concepts or topics, ensuring robust comprehension of the material before progressing to the subsequent module.

However, online learning poses challenges regarding user retention. Although retention rates fluctuate across programs and courses, it is often posited that dropout rates for online courses surpass those of traditional face-to-face courses. (Ali & Leeds, 2009) Feedback from cybersecurity professionals intimates that to counter these challenges, online learning platforms ought to offer learners opportunities for interactive discussions, feedback, and collaboration. Instructors can incorporate resources such as discussion forums and group assignments to stimulate engagement and interaction among learners.

Moreover, instructors can provide personalised feedback to learners, catering to their individual learning needs and aiding in better retention of the material. While emotional support is crucial for retention in an online environment, a certain level of familiarity with the course's logistics also holds significant importance. (Fried, 2007)

5.3.3 *Is Online learning effective at teaching cybersecurity skills?*

The respondents posited that the efficacy of online training ought to be evaluated based on the practical application of skills acquired from the training. This insinuates that the retention of skills learned via online training is best appraised when these skills are applied to day-to-day operations and strategic activities, thereby imparting tangible value to the organisation.

This emphasis on practical application reveals that the respondents place a high value on the practical relevance of learned skills, which can lead to enhanced retention of knowledge and skills. By stressing the practical application of skills acquired through online training, cybersecurity professionals are more likely to

retain and utilise these skills in their work, thereby augmenting effectiveness and value for their organisations.

Moreover, the respondents maintain that an effective online training program is clear and concise regarding its objectives. A potent online learning program must address the attendance of the learner, the course content, communication and collaboration, and the responsibilities of the facilitator and the learner (Fried, 2007)

It's noteworthy that online learning platforms can foster the retention of knowledge and skills by providing learners with access to a diversity of resources, such as online discussion forums, virtual simulations, and other interactive tools. These resources can assist learners in applying their skills across a spectrum of real-world scenarios, thereby helping to reinforce the concepts and techniques absorbed during the training.

5.4 Bandura’s Social Learning Construct – Reproduction

The principle of reproduction in Bandura's social learning theory accentuates that individuals must be capable of reproducing the observed behaviour or skill to learn and apply it in the future. This construct is a dependent one, directly correlated to the Attention and Retention constructs. Consequently, the emphasis is on the learner's ability to reproduce the skills and competencies acquired through the Attention and Retention constructs.

5.4.1 *Which learning format do cybersecurity professionals prefer?*

Within the scope of cybersecurity training, this implies that for the training to be effective, participants must be able to apply the knowledge and skills derived from their training programmes to their daily tasks. This viewpoint aligns with the (Chen, 2014) assertion that fostering critical thinking and practical application of knowledge is one of the key requisites of online learning.

The study's findings suggest that the participants considered the ability to reproduce learned content to be of utmost importance. Overall, the successful

application of knowledge and skills acquired from cybersecurity training programmes by the participants is a pivotal determinant of the training's effectiveness.

5.4.2 *What are the strengths and weaknesses of online learning?*

Based on the analysis, it appears that online learning offers cybersecurity professionals the benefit of practising and applying what they have learned in a safe and controlled environment. Online learning platforms provide cybersecurity professionals with a range of opportunities to complete quizzes, assignments, and projects that allow them to apply their knowledge and receive immediate feedback and support.

The benefit of this approach is that professionals can experiment with different approaches and techniques without the risk of negative consequences. In a traditional classroom environment, the consequences of mistakes can be more significant, potentially resulting in lower grades or missed opportunities. Moreover, the consequences of mistakes with on-the-job training are even worse. Online learning allows cybersecurity professionals to make mistakes, learn from them, and apply their newfound knowledge to real-world scenarios.

Moreover, online learning platforms also offer a range of interactive simulations and virtual labs that enable learners to practice complex skills and techniques. These tools provide a high level of realism and allow cybersecurity professionals to gain practical experience without the need for expensive equipment or facilities.

5.4.3 *Is Online learning effective at teaching cybersecurity skills?*

The analysis discloses that reproduction, or the capability to replicate skills, constitutes a significant facet of online learning effectiveness for cybersecurity professionals. The respondents presented varying perspectives on the measures of the effectiveness of online training within their respective sub-domains but universally concurred that the application of skills acquired during the training is pivotal.

This suggests that the respondents held the belief that online training could effectively instil skills that can be applied to daily operations and strategic activities within their sub-domains. In simpler terms, online learning can equip cybersecurity professionals with the skills required to execute their tasks effectively.

It's noteworthy that online learning platforms can expedite the development of skills by providing learners with opportunities to apply their knowledge in simulated environments, engage in problem-solving activities, and collaborate with peers on real-world projects. These activities can assist learners in building practical skills and bolstering confidence in their ability to apply their knowledge to real-world situations.

5.5 Bandura's Social Learning Construct – Motivation

The final construct emphasizes the motivation of learners to persevere with ongoing tasks. The principle of motivation proposed by Bandura underscores the importance of an individual's aspiration and determination to learn and implement new skills.

5.5.1 *Which learning format do cybersecurity professionals prefer?*

Within the realm of cybersecurity training, the principle of motivation posits that individuals who demonstrate a drive to learn and enhance their abilities are more likely to thrive in the cybersecurity domain. This perspective is corroborated by (Keith S. Jones et al., 2018), who affirm that maintaining self-motivation, curiosity, and interest are pivotal factors.

The findings of the study indicate that participants displayed a high degree of motivation to acquire and hone their skills, as substantiated by their participation in multiple training programs and their predilection for certain training formats. This motivation probably originates from an acknowledgement of the swiftly evolving cybersecurity landscape, necessitating continual education to keep abreast of novel threats and technologies. This notion aligns with the (Blazic, 2021) argument that the quick progression of cybersecurity attacks, coupled with

academia's static nature, has led to growing discrepancies between the knowledge imparted in educational programs and the skills sought by employers — a reality of which cybersecurity professionals are cognizant.

Respondent 6's preference for online, self-paced training underscores further the role of motivation within the learning process. This modality enables individuals to learn at a comfortable pace and concentrate on areas requiring improvement, potentially bolstering their drive to persist in learning and skill enhancement. The principle of motivation underscores the necessity of fostering a learning environment conducive to individual motivation, potentially leading to heightened performance and success within the cybersecurity domain.

5.5.2 *What are the strengths and weaknesses of online learning?*

According to the analysis, one of the strengths of online learning is its capacity to empower learners, granting them a sense of control over their educational journey. Online learning platforms afford learners the flexibility to work at their own pace and engage with materials germane to their interests and objectives. These observations align with (Zhu et al., 2020), who assert that online learning more effectively accommodates the varied needs of students. This degree of flexibility and customization can significantly boost learner motivation, facilitating personal ownership of the learning process and the tailoring of experiences to meet unique requirements.

In contrast, traditional classroom environments often place constraints on learners, offering limited control over the pace and content of instruction, potentially leading to disengagement and diminished motivation. Such settings typically adhere to an imposed-pace model, establishing definitive parameters for the course and mandating uniform engagement in learning activities at specific times (Rhode, 2009)

Online learning, however, opens opportunities for learners to take the reins of their own educational experience, concentrating on the areas they deem most essential.

Additionally, online learning platforms often equip learners with a variety of tools and resources designed to enrich their learning experiences, including interactive quizzes, videos, and other multimedia content. (Rhode, 2009) supports this observation, suggesting that these tools enable a unique exploration of learner preferences, fostering different types of interactions via various online communication tools.

Learners can access these resources at any time, which allows for the review and reinforcement of key concepts as required.

Nevertheless, it is crucial to acknowledge that the level of control and flexibility offered by online learning can pose challenges for learners who grapple with self-regulation and time management. In the absence of the structure and accountability found in a traditional classroom setting, some learners may struggle to sustain motivation and manage their time effectively, thus posing a challenge to invoke and maintain student engagement, ensure comprehension, and foster positive learning outcomes (Myers et al., 2014)

5.5.3 *Is Online learning effective at teaching cybersecurity skills?*

The findings underscore that motivation plays a pivotal role in the efficacy of online learning for cybersecurity professionals. The respondents concurred in their endorsement of online training as an effective means of skill development within their respective sub-domains, suggesting a strong motivation to learn and enhance their abilities via online training.

This discovery accentuates the potential motivational advantages of online learning for cybersecurity professionals. Online learning platforms offer learners flexibility concerning when and where they can study, as well as access to a broad spectrum of materials and resources that can be personalized to align with their interests and objectives. Such features can bolster learners' motivation by granting them control over their educational journey and facilitating the pursuit of their interests and goals.

Furthermore, online learning platforms can present learners with opportunities to partake in interactive and collaborative activities, fostering a sense of community and enhancing motivation. For instance, learners may engage in online forums, discussion boards, and group projects, fostering a sense of camaraderie and motivation.

5.6 Conclusion

In conclusion, online learning provides a flexible and accessible approach to acquiring cybersecurity skills and knowledge. However, it is important to address potential drawbacks associated with the lack of physical interaction and engagement. Instructors should incorporate interactive discussions, provide timely feedback and support, and create a sense of community among learners to mitigate these challenges. Retention and practical application of skills are important factors to consider when evaluating the effectiveness of online learning, and online learning platforms can provide learners with access to a range of resources and tools to facilitate this. Furthermore, self-regulation and time management skills are critical for successful online learning, and online learning platforms should provide learners with the necessary tools and support. Overall, online learning can be a motivating approach for cybersecurity professionals to develop their skills and foster a lifelong love of learning.

CHAPTER 6. CONCLUSION

6.1 Introduction

This chapter provides a conclusion to the research, offers recommendations based on the results, and suggests directions for future research.

The study investigated the role of online learning in addressing the shortage of cybersecurity skills within the South African financial services sector. It examined the preferred learning formats of cybersecurity professionals, identified the strengths and weaknesses of online learning, and assessed the efficacy of online learning in imparting cybersecurity skills.

The principles of attention, retention, and motivation in cybersecurity training were discussed in the study. It underscored the importance of attending to training stimuli, devising training programs that capture the attention of individuals, and accommodating their attentional preferences. The findings demonstrated that different training formats, such as physical on-the-job training, physical classroom training, and online training, impact attention and engagement differently.

Participants exhibited individual preferences for different formats, with the majority favouring online self-paced training and physical classroom training. The study also emphasized the importance of retention in cybersecurity training, as professionals must retain and recall knowledge and skills for effective application. Continuous training is crucial to keep pace with the rapidly evolving nature of the field. Finally, the principle of motivation suggests that those who are driven to learn and apply their skills are more likely to thrive in the field of cybersecurity. The motivation of participants was apparent through their participation in multiple training programs and their preference for specific formats.

6.2 Key Takeaways

Attention: The principle of attention implies that learning ensues when learners focus on the behaviour of others. In the context of online learning, employing multimedia, interactive tools, and gamification can heighten learners' attention and engagement. Nevertheless, distractions originating from social media and other online platforms may negatively influence attention and focus, leading to diminished learning outcomes.

Retention: Retention pertains to the ability to store and recall absorbed information. Online learning can afford opportunities for learners to review and revisit content according to their pace, thereby enhancing retention. However, the absence of personal interaction and instructor feedback may contribute to a decline in the retention and application of knowledge.

Reproduction: The principle of reproduction contends that learning transpires when learners replicate observed behaviour. Online learning can present opportunities for learners to practice and apply knowledge via simulations, virtual labs, and online discussions. Yet, without the physical presence of an instructor, learners may lack the necessary guidance and feedback to effectively reproduce desired behaviours.

Motivation: Motivation signifies the impetus to learn and achieve goals. Online learning can provide flexibility, convenience, and access to a diverse range of resources, thereby boosting learner motivation. However, a lack of social interaction and community building could lead to decreased motivation and engagement.

6.3 Recommendations

Through the study, we could identify some key considerations to ensure that online learning is effective at teaching cybersecurity skills. In this section, we look at some recommendations that could contribute to ensuring the effectiveness of cybersecurity learning:

1. Tailor online training programs to individual attentional preferences: Develop training programs that cater to diverse learner preferences. This customization can improve participants' attention and engagement, leading to better knowledge retention and practical application.

2. Implement blended learning approaches: Combine different training formats, such as online self-paced modules, online instructor-led sessions, and hands-on practical exercises, to create a blended learning environment. This approach can provide flexibility, interactivity, and real-world application, maximizing participants' attention, retention, and motivation.

3. Incorporate active learning strategies: Integrate active learning techniques, such as case studies, group discussions, problem-solving activities, and simulations, into cybersecurity online training programs. These strategies promote engagement, critical thinking, and practical application of knowledge, enhancing retention and skill development.

4. Foster a collaborative learning environment: Encourage collaboration and interaction among participants through online forums, peer-to-peer mentoring, and networking opportunities. This collaborative environment can enhance motivation, knowledge sharing, and the development of practical skills through experiential learning.

5. Emphasize practical application and real-world scenarios: Design training programs that prioritize hands-on experiences and practical application of knowledge in real-world cybersecurity scenarios. This approach helps participants bridge the gap between theoretical knowledge and practical skills, facilitating retention and preparing them for the challenges they may encounter in their professional roles.

By implementing these recommendations, cybersecurity training programs can be designed and executed in a manner that optimizes attention, retention, and motivation. This will ultimately contribute to the development of highly skilled and

competent cybersecurity professionals capable of addressing the complex challenges of the digital landscape.

6.4 Suggestions for further research

Research on how online learning can be used to upskill cybersecurity professionals is an important area of study considering the increasing demand for skilled cybersecurity experts. Here are some suggestions for further research:

1. Effectiveness of online learning platforms: Investigate the effectiveness of different online learning platforms in delivering cybersecurity training. Compare various platforms in terms of content quality, engagement, hands-on exercises, and the ability to cater to technical and non-technical skills.
2. Gamification and interactive learning: Explore the impact of gamification and interactive elements in online cybersecurity courses. Examine how gamified elements such as badges, leaderboards, and virtual labs can enhance learning outcomes and motivate professionals to upskill.
3. Adaptive learning and personalized training: Investigate the effectiveness of adaptive learning techniques in online cybersecurity training. Explore how personalized training paths, based on learners' existing knowledge and skill gaps, can improve learning efficiency and retention.
4. Collaborative learning and community engagement: Study the impact of collaborative learning approaches in online cybersecurity training. Explore how features like discussion forums, peer assessments, and group projects can foster knowledge sharing, collaboration, and the development of problem-solving skills.

These research areas can provide valuable insights into leveraging online learning to upskill cybersecurity professionals and meet the growing demands of the industry.

REFERENCES

Ali, R., & Leeds, E. M. (2009). The impact of face-to-face orientation on online retention: A pilot study. *Online Journal of Distance Learning Administration, 12*(4).

Anderson, R. (2007). Thematic Content Analysis- Descriptive Presentation of Qualitative Data

Blazic, B. (2021). The cybersecurity labour shortage in Europe: Moving to a new concept for education and training. Retrieved from https://www.sciencedirect.com/science/article/pii/S0160791X2100244X

Cashell, B., Jackson, W. D., Jickling, M., & Webel, B. (2004). The economic impact of cyber-attacks. *Congressional research service documents, CRS RL32331 (Washington DC), 2*.

Chen, S.-J. (2014). Instructional design strategies for intensive online courses: An objectivist-constructivist blended approach. *Journal of interactive online learning, 13*(1).

Collins, J. (1982). Discourse style, classroom interaction and differential treatment. *Journal of reading behavior, 14*(4), 429-437.

Cook, D. A., & Smith, A. J. (2006). Validity of index of learning styles scores: multitrait− multimethod comparison with three cognitive/learning style instruments. *Medical education, 40*(9), 900-907.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review, 4*(10).

Creswell, J. (2013). Qualitative Inquiry and Research Design. *3e*.

Creswell, J. W. (2014). Research Design: Qualitative, Quantitative and Mixed Methods Approaches. *4e*.

Cybersecurity, E. U. A. f. (2019). *ENISA threat landscape report 2018 : 15 top cyber-threats and trends*: European Network and Information Security Agency.

de Freitas, S. I., Morgan, J., & Gibson, D. (2015). Will MOOCs transform learning and teaching in higher education? Engagement and course retention in online learning provision. *British journal of educational technology, 46*(3), 455-471. doi:10.1111/bjet.12268

Dhawan, S. (2020). Online Learning: A Panacea in the Time of COVID-19 Crisis. *Journal of Educational Technology Systems, 49*(1), 5-22. doi:10.1177/0047239520934018

Fortinet. (2022). 2022 Cybersecurity Skills Gap. *Global Research Report*.

Fried, J. (2007). Learning communities as learning systems. Journal of Learning Communities Research.

Furnell, S. (2020). The cybersecurity workforce and skills. Retrieved from https://www.researchgate.net/publication/346303382_The_cybersecurity_workforce_and_skills

Garrison, D. R., & Vaughan, N. D. (2008). *Blended learning in higher education: Framework, principles, and guidelines*: John Wiley & Sons.

ISC2. (2019). Strategies for Building and Growing Strong Cybersecurity Team. *(ISC)2 CYBERSECURITY WORKFORCE STUDY, 2019*. Retrieved from https://www.isc2.org/Research/2019-Cybersecurity-Workforce-Study

ISC2. (2021). A Resilient Cybersecurity Profession Charts the Path Forward. *(ISC)2 Cybersecurity Workforce Study, 2021*, 3. Retrieved from https://www.isc2.org/Research/Workforce-Study

Johnson, S. L. (2010). A question of time: Cross-sectional versus longitudinal study designs. *Pediatrics, 31*, 250-251.

Jung, I. (2019). Advantages and Limitations of Online Learning in Higher Education: An Empirical Study.

Kamble, A., Gauba, R., Desai, S., & Golhar, D. (2021). Learners' perception of the transition to instructor-led online learning environments: Facilitators and barriers during the COVID-19 pandemic. *International Review of Research in Open and Distributed Learning, 22*(1), 199-215.

Keith S. Jones, Akbar Siami Namin, & Miriam E. Armstrong. (2018). The Core Cyber-Defense Knowledge, Skills, and Abilities That Cybersecurity Students Should Learn in School: Results from Interviews with Cybersecurity Professionals.

LaMorte, W. (2019). The Social Cognitive Theory. Retrieved from https://sphweb.bumc.bu.edu/otlt/MPH-Modules/SB/BehavioralChangeTheories/BehavioralChangeTheories5.html

McGettrick, A., Cassel, L., Dark, M., Hawthorne, E., & Impagliazzo, J. (2014). *Toward curricular guidelines for cybersecurity*.

McLeod, S. (2011). Albert Bandura's social learning theory.

Mincer, J. (1962). On-the-job training: Costs, returns, and some implications. *Journal of political Economy, 70*(5, Part 2), 50-79.

Moore, J. L., Dickson-Deane, C., & Galyen, K. (2011). e-Learning, online learning, and distance learning environments: Are they the same? *The Internet and higher education, 14*(2), 129-135. doi:https://doi.org/10.1016/j.iheduc.2010.10.001

Myers, T., Blackman, A., Andersen, T., Hay, R., Lee, I., & Gray, H. (2014). Cultivating ICT students' interpersonal soft skills in online learning environments using traditional active learning techniques. *Journal of Learning Design, 7*, 38-53.

Nickerson, C. (2022). Social Cognitive Theory: How We Learn From the Behavior of Others. Retrieved from https://www.simplypsychology.org/social-cognitive-theory.html

Oltsik, J., & Lundell, B. (2021). The Life and Times of Cybersecurity Professionals 2021. *ESG Research Report, 5*. Retrieved from https://www.esg-global.com/research/esg-research-report-the-life-and-times-of-cybersecurity-professionals-2021-volume-v

Rhode, J. (2009). Interaction equivalency in self-paced online learning environments: An exploration of learner preferences. *The international review of research in open and distributed learning, 10*(1).

Sandelowski, M. (1986). The problem of rigor in qualitative research. *Advances in Nursing Science, 8*(3), 27-37. Retrieved from https://journals.lww.com/advancesinnursingscience/Fulltext/1986/04000/The_problem_of_rigor_in_qualitative_research.5.aspx

Shuell, T. J. (2001). Teaching and Learning in the Classroom. In N. J. Smelser & P. B. Baltes (Eds.), *International Encyclopedia of the Social & Behavioral Sciences* (pp. 15468-15472). Oxford: Pergamon.

SkillSoft. Cybersecurity Glossary Of Terms. Retrieved from https://www.globalknowledge.com/us-en/topics/cybersecurity/glossary-of-terms/#gref

Švábenský, V., ˇCeleda, P., Vykopal, J., & Brišáková, S. (2020). Cybersecurity knowledge and skills taught in capture the flag challenges.

Thesaurus, C. A. L. s. D. (Ed.).

ThroughEducation. (2019). Everything You Need To Know About Formal Education. Retrieved from https://www.throughеducation.com/everything-you-need-to-know-about-formal-education/

Tracy, S. J. (2010). Qualitative Quality: Eight “Big-Tent” Criteria for Excellent Qualitative Research. *Qualitative inquiry, 16*(10), 837-851. doi:10.1177/1077800410383121

Zhu, Y., Zhang, J. H., Au, W., & Yates, G. (2020). University students’ online learning attitudes and continuous intention to undertake online courses: a self-regulated learning perspective. *Educational technology research and development, 68*(3), 1485-1519. doi:10.1007/s11423-020-09753-w

APPENDIX A Participant information sheet

Dear Sir / Madam

My name is Lefa Kgosiatsela, and I am a Masters' student in Digital Business at the University of the Witwatersrand, Johannesburg. As part of my studies, I have to undertake a research project, and I am investigating online learning and its role in addressing the cybersecurity skills shortage in South Africa under the supervision of Dr Kiru Pillay. This research project aims to find out how online learning can be used effectively to assist in training cybersecurity professionals, and thus assist in decreasing the skills shortage in the South African Financial Services industry.

As part of this project, I would like to invite you to take part in an interview. This activity will involve a discussion over MS Teams and will take around 20 minutes. With your permission, I would also like to audio record the interview using a digital device. This recording will be stored in an encrypted hard drive and only the researcher will have access to this recording. It will be deleted after the research has been concluded.

There will be no personal costs to you if you participate in this project, You will not receive any direct benefits from participation but there are no disadvantages or penalties if you do not choose to participate or if you withdraw from the study. You may withdraw at any time or not answer any questions if you do not want to. The interview will be completely confidential and anonymous as I will not be asking for your name or any identifying information, and the information you give to me will be held securely and not disclosed to anyone else. I will be using a pseudonym (false name) to represent your participation in my final research report. If you experience any distress or discomfort at any point in this process, we will stop the interview or resume another time.

If you have any questions during or afterwards about this research, feel free to contact me on the details listed below. This study will be written up as a research report which will be available online through the university library website. If you wish to receive a summary of this report, I will be happy to send it to you

(optional). The data collected from this research project will be stored in an encrypted hard drive and will be kept until the research is concluded. With your permission, the data collected from this research project may be used by other researchers in an anonymized format. If you have any concerns or complaints regarding the ethical procedures of this study, you are welcome to contact the University Human Research Ethics Committee (Non-Medical), telephone +27(0) 11 717 1408, email hrecnon-medical@wits.ac.za

Yours sincerely,

Lefa Kgosiatsela

Researcher:

Lefa Kgosiatsela, 2412173@students.wits.ac.za,

Supervisor:

Dr Kiru Pillay

APPENDIX B Participant agreement form

Title of project: Investigating online learning and its role in addressing the cybersecurity skills shortage in South Africa

Name of researcher: Lefa Kgosiatsela

I, ..., agree to participate in this research project. The research has been explained to me and I understand what my participation will involve. I agree to the following:

(Please circle the relevant options below).

I agree that my participation will remain anonymous	YES	NO
I agree that the researcher may use anonymous quotes in his / her research report	YES	NO
I agree that the interview may be audio recorded	YES	NO
I agree that the information I provide may be used anonymously after this project has ended, for academic purposes by other researchers, subject to their own ethics clearance being obtained.	YES	NO

... (signature of participant)

... (name of participant)

... (date)

... (signature of the researcher)

... (name of the person seeking consent)

... (date)

APPENDIX C Instrument

Dear Respondent,

My name is **Lefa Kgosiatsela**. I am a **Master of Management in Digital Business** (MMDB) student at **Wits Business School** (WBS).

As part of my studies, I must undertake a research project. I am conducting research on **'Investigating online learning and its role in addressing the cybersecurity skills shortage in South Africa'** under the supervision of **Dr Kiru Pillay**. The purpose of the study is to evaluate how online learning can be used effectively to assist in training cybersecurity professionals, and thus assist in decreasing the skills shortage in the South African Financial Services industry.

I kindly request your assistance in taking part in an interview to contribute to the outcome of the study and the completion of my master's degree. Please supply proof of consent by replying to the email allowing me to go ahead with the interview.

About interview:

- Taking part in the interview process is voluntary.
- You may stop the interview process at any stage.
- There are no personal identifiers or personal information collected therefore your identity will remain completely anonymous.
- The data collected will be kept confidential.
- It should take approximately 20 minutes to complete all the questions.

Please feel free to contact me if you have any questions about this research project, on the contact details given below.

If you have any concerns or complaints regarding the ethical procedures of this study, you are welcome to contact the University Human Research Ethics Committee (Non-Medical) at +27 11 717 1408 or hrecnonmedical@wits.ac.za.

Thanking you in advance.

Yours sincerely,

Lefa Kgosiatsela

Researcher: Lefa Kgosiatsela

Email: 2412173@students.wits.ac.za

Mobile: +27 71 860 9702

Interview Questions

Research Question 1: Which learning format do cybersecurity professionals prefer?

Research Instrument Questions:

1. In what format were these training programs delivered? Was it through?
    - On-the job-training,
    - Classroom style training
    - Online learning
    - Other?
2. Of the four options in which you got training, which one do you prefer for your specific sub-domain and why?

Research Question 2: What are the strengths and weaknesses of online learning?

Research Instrument Questions:

1. Can you provide your experience on each of the cyber training you completed?
2. What did you enjoy the most about the training?
3. What did you enjoy the least about the training?
4. In your opinion, what are some key things to consider when it comes to online training for your specific sub-domain? And why?
5. Focusing on online training, what are some of the strengths & weaknesses of online training when it comes to your specific sub-domain? And why?

Research Question 3: Is Online learning effective at teaching cybersecurity skills?

Research Instrument Questions:

1. In your opinion, do you think there are elements of technical training that can be provided effectively online? i.e., Pen testing, configuration, etc.
2. In your opinion, do you think there are elements of non-technical training that can be provided effectively online? i.e., Cyber policy writing skills, cyber risk?
3. What are some measures of effectiveness when it comes to training for your subdomain?
4. In your opinion is online training effective at training skills in your respective Cybersecurity speciality? Please provide reasons.