



Recommendations for cybersecurity awareness for the South African local government using a gamification approach

GP Hlungwani



[orcid.org/ 0000-0003-3932-0100](https://orcid.org/0000-0003-3932-0100)

Dissertation accepted in fulfilment of the requirements for the degree *Master of Science in Computer Science* at the North-West University

Supervisor: Prof V Malele

Graduation: May 2026

ACKNOWLEDGEMENTS

Firstly, I glorify the God of Mount Zion for the direction, blessing, and strength that have been my foundation throughout this journey. I would like to express my profound gratitude to my mother for her constant support and confidence in my abilities. I want to express my gratitude to my two spouses, Tsakani and Mercy Hlungwani, for their love, patience and encouragement during this journey. I thank my supervisor, Professor Vusumuzi Malele, for his helpful advice and guidance, which has had a major positive impact on my research. Furthermore, I am truly grateful to North-West University for providing me with essential tools, platforms and funding that have helped me develop my academic and personal life.

DECLARATION

I, Giyani Phanuel Hlungwani, declare that the master's dissertation titled "Recommendations for cybersecurity awareness for the South African local government using a gamification approach" is my own work and that all the sources I have used or cited are given complete references.

Table 1-1: Declaration

Approval	Student	Supervisor
Signature		
Date	26 November 2025	27 November 2025

ABSTRACT

Although most cases of cybersecurity challenges are reported by large private organisations, it should be noted that public organisations are not immune. For example, in recent years, several government departments have experienced cyber-attacks and threats. The latter created a cybersecurity risk that needed to be addressed.

The main aim of this study was to make recommendations for cybersecurity awareness using gamification approach for South African local government. This study was guided by three theoretical frameworks: (i) Cybersecurity Frameworks (CSF), (ii) Line-of-Defence (LoD), and (iii) Gamification. To achieve the main aim, several objectives (subdivided into primary and secondary) were put into place.

Due to the nature of this study, an action research case study research methodology with a focus on local government was adopted. It was implemented using structured methods for data collection, analysis (drawing patterns), and development of recommendations. In this regard, the researcher conducted a literature review using different techniques, field research, and a qualitative interpretation case study approach. Action research was carried out using three phases.

In the first phase of this study, the contextualisation and interaction process was used through a systematic literature review (SLR) aimed at exploring existing cybersecurity strategies and frameworks related to local governments. Furthermore, a selection of an appropriate game tool was made to promote gamification by collecting rich contextual data during game play to improve awareness of cybersecurity in the local government was conducted.

The second phase, ‘Abstract and Reasoning’, focuses on critically assessing the selection of appropriate research methods to understand the unique cybersecurity challenges facing local governments. The objective of this phase was to develop a theoretical view of how local government employees perceive and react to cybersecurity threats and to formulate literature recommendations for gamification awareness. In this regard, a brief survey using questionnaires was conducted.

The third phase, ‘Multiple Interpretations and Suspicions’, allowed local government employees to formulate focus groups that were exposed to different experimental processes. In this regard, semi-structured interviews were used as a form of collecting employee knowledge, perception, and adoptability of the cybersecurity strategy using gamifications. The quality data from the focus group meetings was analysed and synthesised to produce recommendations. In this regard, content analysis was used to extract meaningful patterns and insights that were used. Furthermore, semi-structured interviews were used to validate the draft recommendations which were also compared to literature.

Results indicated that gamification significantly improves engagement and retention of cybersecurity practices. Employees exposed to game-based learning demonstrated higher motivation and adaptability, suggesting that gamification can effectively bridge the gap between theory and practice. This study recommended integrating gamified modules into existing cybersecurity programmes, developing localised framework aligned with national standards, and implementing continuous monitoring and feedback. Policy support and resource allocation are essential for sustainability.

This research was limited to a single local government, which may affect generalisability. Future studies should include multiple local governments and examine the long-term impact of gamification-based training.

Keywords: Cybersecurity Awareness; Gamification; Local Government; Action Research; Cybersecurity Frameworks; Line-of-Defence; South Africa

Abbreviations and Acronyms

Abbrev.	Pg.	Abbrev.	Pg.
Advanced Persistent Threats (APT)	11	Information Security Management System (ISMS)	21
African Cybersecurity Research Institute (ACRI)	8	Information Systems Audit and Control Association (ISACA)	22
Centre for Internet Security (CIS)	25	International Business Machines Corporation (IBM)	12
Chief Executive Officer (CEO)	11	International Organisation for Standardization (ISO)	21
Chief Information Officer (CIO)	12	Internet of Things (IoT)	12
Chief Information Security Officer (CISO)	12	Intrusion detection systems (IDS)	62
City of Johannesburg (CoJ)	1	Klynveld Peat Marwick Goerdeler (KPMG)	14
Cloud Controls Matrix (CCM)	23	Learning Management Systems (LMS)	71
Common Security Framework (CSF)	22	Lines-of-Defence (LoDs)	iv
Confidentiality, Integrity, and Availability (CIA triad)	18	Man-in-the-Middle (MitM)	14
Control Objectives for Information and Related Technologies (COBIT)	22	National Cyber Security Centre (NCSC)	12
Cybersecurity Capacity Centre for Southern Africa (C3SA)	10	National Institute of Standards and Technology (NIST)	16
Cybersecurity Framework (CFS)	iv	Payment Card Industry Data Security Standard (PCI-DSS)	21
Cybersecurity Maturity Model (CMMC)	23	Points, badges, and Leaderboards (PBL)	70
Data Loss Prevention (DLP)	9	PricewaterhouseCoopers (PWC)	12
Denial of service (DoS)	11	Primary objectives (PO)	4
Distributed Denial of Service (DDoS)	11	Protection of Personal Information Act (POPIA)	14
Electronic Protected Health Information (ePHI)	54	Role-based access control (RBAC)	63
Empirical objectives (EO)	4	Secondary objectives (SO)	4
European Union Agency for Cybersecurity (ENISA)	59	security information and event management	

		(SIEM)	1
Federal Bureau of Investigation (FBI)	11	Service Organisation Control (SOC)	26
First Line-of-Defence (LoD 1)	1	South African Local Government Association (SALGA)	33
C Framework (Change, Compliance, Cost, Continuity, and Coverage)	20	Structured Query Language	14
General Data Protection Regulation (GDPR)	54	SysAdmin, Audit, Network, and Security SANS	12
Health Insurance Portability and Accountability Act (HIPAA)	54	systematic literature review (SLR)	iv

TABLE OF CONTENTS

ACKNOWLEDGEMENTS	I
DECLARATION.....	II
ABSTRACT	III
ABBREVIATIONS AND ACRONYMS	V
CHAPTER 1.....	1
INTRODUCTION	1
1.1 BACKGROUND.....	1
1.2 LITERATURE REVIEW.....	3
1.3 SIGNIFICANCE OF THE STUDY.....	6
1.4 PROBLEM STATEMENT.....	7
1.5 STUDY AIM AND OBJECTIVES.....	8
1.6 STUDY RESEARCH PROCEDURE.....	9
1.7 STUDY CONTRIBUTION	10
1.8 CHAPTER LAYOUT	10
1.9 CONCLUSION	12
CHAPTER 2.....	13
METHODOLOGY	13
2.1 INTRODUCTION	13
2.2 RESEARCH PHILOSOPHY.....	14
2.3 RESEARCH DESIGN	16
2.4 RESEARCH METHODS	17
2.5 RESEARCH ENVIRONMENT.....	18
2.6 POPULATION AND SAMPLE SIZE	19
2.7 DATA COLLECTION	21
2.7.1. SCOPING AND SYSTEMATIC LITERATURE REVIEW	21
2.7.2. EMPIRICAL DATA COLLECTION TECHNIQUES	24
2.8 RESEARCH TOOLS	25
2.9 ETHICAL PROTOCOL.....	28
2.10 VALIDITY AND RELIABILITY.....	28
2.11 CONCLUSION	28
CHAPTER 3.....	29
FINDINGS: SCOPING LITERATURE REVIEW	29

3.1 INTRODUCTION	29
3.2 CYBERSECURITY THREATS AND ATTACKS	29
3.3 CYBERSECURITY RISKS AND VULNERABILITIES.....	39
3.4 CYBERSECURITY THEORIES, MODELS AND FRAMEWORKS.....	43
3.5 CYBERSECURITY BEST PRACTICES	53
3.6 RECOMMENDATION	59
3.7 CYBERSECURITY STRATEGIES	60
3.8 RECOMMENDATION	66
3.9 CONCLUSION	67
CHAPTER 4.....	69
FINDINGS: SYSTEMATIC LITERATURE REVIEW	69
4.1 INTRODUCTION	69
4.2 IDENTIFY AND SELECT CYBERSECURITY GAMES THAT ARE SUITABLE FOR THE SPECIFIC CONTEXT OF THE CYBERSECURITY AWARENESS CONTEXT	70
4.3 DESIGN CONSIDERATIONS AND VALIDATION METHODS FOR THE DEVELOPMENT AND USAGE OF CYBERSECURITY AWARENESS STRATEGIES USING GAMIFICATION	74
4.4 GAMIFICATION TOOLS	81
4.5 RECOMMENDATION	85
4.6 CONCLUSION	87
CHAPTER 5.....	89
EMPIRICAL FINDINGS	89
5.1 INTRODUCTION	89
5.2 FOCUS GROUP ANALYSIS.....	90
5.3.1 THEME 1: KNOWLEDGE OF CYBERSECURITY IN LOCAL GOVERNMENT	92
5.3.2 THEME 2: CONFIDENCE AROUND CYBERSECURITY WITHIN LOCAL GOVERNMENTS	94
5.3.3 THEME 3: CONCEPTS AND AREAS OF CYBERSECURITY LEARNT IN PLAYING THE GAME	95
5.3.4 THEME 4: APPLICABILITY OF CYBERSECURITY KNOWLEDGE IN REAL-LIFE SITUATIONS.....	96
5.3 INTERVIEWS.....	98
5.4.1 THEME 5: PERCEPTIONS ABOUT CYBERSECURITY KNOWLEDGE.....	98
5.4.2 THEME 6: ENHANCEMENT OF CYBERSECURITY UNDERSTANDING	101
5.4.3 THEME 7: CAPACITY OF THE LOCAL GOVERNMENT TO IMPLEMENT GAMIFICATION TO IMPROVE CYBERSECURITY KNOWLEDGE.....	102
5.4 RECOMMENDATIONS	103
5.5 CONCLUSION	104
CHAPTER 6.....	105

CONTRIBUTIONS.....	105
6.1 INTRODUCTION	105
6.2 RECOMMENDATION 1: MULTILAYERED DEFENCE APPROACH	105
6.3 RECOMMENDATION: SOUTH AFRICAN REGULATORY FRAMEWORK.....	107
6.4 RECOMMENDATION: THIRD-PARTY MONITORING.....	108
6.5 RECOMMENDATIONS FOR FORMULATING A CYBERSECURITY AWARENESS STRATEGY THROUGH GAMIFICATION	109
6.6 RECOMMENDATIONS FOR A GOOD CYBERSECURITY AWARENESS GAME RELEVANT FOR THE LOCAL GOVERNMENT SETTING	112
6.7 RECOMMENDATIONS FOR AN IMPLEMENTATION STRATEGY OF A GOOD CYBERSECURITY AWARENESS GAME RELEVANT FOR THE LOCAL GOVERNMENT SETTING	113
6.8 RECOMMENDATIONS FOR LACK OF KNOWLEDGE ON CYBER THREATS	113
6.9 CONCLUSION	114
CHAPTER 7.....	117
LESSON LEARNT	117
7.1 INTRODUCTION	117
7.2 CHALLENGES AND OPPORTUNITIES ENCOUNTERED DURING LITERATURE REVIEW.....	117
7.3 CHALLENGES AND OPPORTUNITIES ENCOUNTERED DURING DATA GENERATION	118
7.4 CONCLUSION	120
CHAPTER 8.....	121
CONCLUSIONS AND FUTURE STUDIES	121
8.1 INTRODUCTION	121
8.2 CONCLUSION	121
8.3 RECOMMENDATIONS FOR FUTURE RESEARCH	122
REFERENCES	123
ANNEXURE A: ETHICS APPROVAL LETTER OF STUDY	151
ANNEXURE B: LETTER OF PERMISSION TO CONDUCT RESEARCH	152
ANNEXURE C: INVITATION TO PARTICIPATE.....	153
ANNEXURE D: CONSENT TO PARTICIPATE.....	154
ANNEXURE E: FOCUS GROUP ATTENDANCE REGISTER	155
ANNEXURE F: CYBERSECURITY AWARENESS QUESTIONNAIRE.....	156

List of Tables

Table 1-1: Declaration	ii
Table 3-1: Summary of possible types of actors, strategies and motivation used in cybercrimes	30
Table 3-2: Comparative Analysis of Cybersecurity Theories	45
Table 3-3: Comparison of Cybersecurity Models	46
Table 3-4: An overview of the cybersecurity frameworks	51
Table 3-5: Summary of cybersecurity best practices	54
Table 3-6: Summary of cybersecurity strategies	61
Table 3-7: Comparison of Cybersecurity Models and Frameworks	66
Table 4-1: A summary of similar studies and identifies gaps	74
Table 4-2: Findings table	79
Table 4-3: Summary of cybersecurity games that could be used in government settings.	82
Table 5-1: Interview Participants biography	90
Table 5-2: Participants codes	91
Table 5-3: Themes	92
Table 5-4: Cybersecurity knowledge before playing the Trivia Twirl Game	93
Table 5-5: Cybersecurity knowledge after playing the Trivia Twirl Game	93
Table 5-6: Confidence Before Playing Trivia Twirl	94
Table 5-7: Confidence After Playing Trivia Twirl	94
Table 5-8: Understanding Before Playing the Game	96
Table 5-9: Understanding After Playing the Game	96
Table 5-10: Participant ratings on Applicability of Cybersecurity Knowledge	97
Table 6-1: Summary of recommendations in alignment to the objectives.	115
Table 7-1: Summary of recommendations in alignment to the objectives.	117

Table 7-2: Summary of recommendations in alignment to the objectives.	119
--	-----

List of Figures

Figure 1-1: Study research procedure (Source: Author, 2024).	9
Figure 2-1: Pillars of research paradigms (Kivunja and Kuyini, 2017)	14
Figure 2-2: The adopted research process (Source: Author).	16
Figure 2-3: Map of Limpopo Province (Source: Municipalities of South Africa).19	
Figure 2-4: The adopted research process (Source: Author).	20
Figure 2-5: PRISMA flow diagram (Source: Author)	24
Figure 2-6: CDSE Cyber Trivia Twirl (Source: CDSE)	26
Figure 2-7: CDSE Cyber Trivia Twirl Quiz (Source: CDSE).....	27
Figure 3-1: Reported phishing incidents in South Africa over five years (SABRIC, 2024).....	31
Figure 3-2: Relationship between Theory, Models, and Frameworks (Source: Author)	43
Figure 3-3: Adoption of cybersecurity models (Hasani et al., 2023)	47
Figure 3-4: Components of the cybersecurity awareness strategy (Source: Author).....	63
Figure 4-1: Components of the cybersecurity awareness strategy (Source: Chapter 2).....	69
Figure 4-2: CDSE Cyber Trivia Twirl (Source: CDSE)	83
Figure 4-3: CDSE Cyber Trivia Twirl Quiz (Source: CDSE).....	84
Figure 5-1: Participant demographic distribution.	91
Figure 5-2: Cybersecurity knowledge before and after playing the game.....	93
Figure 5-3: Confidence in Cybersecurity Before and After Playing Trivia Twirl .95	
Figure 5-4: Applicability of cybersecurity knowledge in real-life situations	97

CHAPTER 1

INTRODUCTION

This chapter introduces this dissertation by discussing the study background, significance, problem statement, aim, research objectives, highlighting the research procedure and the main contributions, and concludes by giving the direction of how this dissertation is structured.

1.1 Background

Cybersecurity has become a major concern for various organisations, especially in the public sector. The public sector is responsible for providing essential services to citizens of the country, especially at local community level. They are the guardians of large amounts of sensitive data, including personal information and important service records.

The growing reliance on digital devices has led to a significant rise in cybersecurity risks. A comprehensive survey conducted in the United States of America found that local governments face persistent and frequent cyberattacks (Norris et al., 2021). Similarly, in 2019, the City of Johannesburg (CoJ), a major metropolitan municipality in South Africa, suffered two serious ransomware incidents: one targeting its electricity supply and another involving a network breach (Pieterse, 2021). These cases highlight the urgent need for local governments to review and strengthen their cybersecurity strategies to better protect against evolving threats.

The growing sophistication of cyber threats poses significant risks to local governments, which requires a comprehensive approach to cybersecurity awareness. Cybercriminals can attack an organisation in a variety of ways, such as man-in-the-middle, brute-force attacks, distributed denial-of-service, malware, phishing, and social engineering (Bendovschi, 2015). To combat cyberthreats and create a cyber-safety environment, organisations need to re-evaluate their cybersecurity strategy. One way of achieving the latter is to deal with the threats that could be enabled by employees such as the Man-in-the-Middle (MITM) attack (i.e., attackers secretly intercept and potentially alter communication between employees or employees and clients). Employees are an essential component of any organisation's first line of defence (LoD), herewith referred to LoD-1, against cybersecurity threats, risks, and attacks (Al-Mohammed

and Baydoun, 2024). LoD-1 consists of operational management, which is responsible for maintaining internal controls and implementing risk procedures. In addition, it adopts a security awareness training strategy to educate employees about best cybersecurity practices and how to recognise phishing and other social engineering attacks. The second LoD (hereafter referred to as LoD-2) focuses on the surveillance, monitoring, and guidance of risk management and compliance. Among other strategies used by LoD-2 is the security information and event management (SIEM) strategy to collect and analyse data from various sources, detect unusual patterns and abnormalities, and provide real-time information and alerts. The third LoD (hereafter referred to as LoD-3) provides independent assurances and advice on the assessments of LoD-1 and LoD-2. One of the cybersecurity strategies used by LoD-3 is external audits and assessments, in which third-party experts are involved in providing independent assessments of cybersecurity postures and identifying potential vulnerabilities. Awareness of cybersecurity is essential in LoD-1 because it can enable employees to recognise and avoid phishing attacks, social engineering tactics, and other cyber threats and minimise human errors (Sharif, 2024).

Cybersecurity awareness is an essential component in building strong defences against cyber threats (Almeida et al., 2017). However, traditional methods for cybersecurity awareness training seem not to be effective because they fail to engage employees effectively (Prümmer et al., 2024). Consequently, it is imperative to adopt innovative approaches that appeal to the target audience. For example, gamification is one such approach. Gamification uses game design elements in nongaming contexts to promote engagement and learning outcomes. Gamification has gained popularity in various sectors, including education and corporate training, to improve user participation and facilitate knowledge acquisition (Nwokeji et al., 2020; Matovu, et al., 2022; Prümmer, 2024; Ahmed et al., 2024).

This study hypothesised that integrating game mechanics to facilitate training of local government employees can promote an environment in which employees can learn about cyber security threats and actively participate in their prevention through interactive and fun activities (Kapp, 2012). The latter could improve the local government's cybersecurity awareness index.

1.2 Literature Review

In this era of digitalisation of processes, there exist many cybersecurity challenges. For example, attempts at penetrating digital devices to elicit, among other things, personal identification information, account data, etc. have been viral (Malele and Mphasane, 2025). Due to the growing reliance on digital devices and infrastructure, cyber threats, attacks, risks, and vulnerabilities affect governments, organisations, and individuals. Rapid digitisation of customer channels, product ecosystems, and organisational operations has made cybersecurity a top national and enterprise priority in South Africa. South Africa is no exception to the global concerns of cybersecurity threats, attacks, vulnerability, and risks. The country's cyberattack surface has grown dramatically as a result of the integration of application programming interface-based systems, the widespread adoption of cloud computing, and the proliferation of mobile technologies.

Further, a cyber-safety environment is significantly important and must always be maintained. To understand and maintain cyber-safety environment within the organisations require to conduct cybersecurity vulnerability, threats and risk analysis. The most common threats that affect African countries, including South Africa, are ransomware, botnets, business email compromise (BEC), and various types of online fraud (Interpol, 2021). The growing use of generative artificial intelligence (AI) tools, which improve the sophistication of identity-based attacks and give phishing campaigns more legitimacy, is adding to this threat landscape (Microsoft, 2024; Hämmäläinen, 2024). These risks have a significant economic impact. The average cost of a data breach in South Africa increased from roughly R49.5 million in 2023 to R53.1 million in 2024, according to IBM's Cost of a Data Breach study. The most common initial attack vectors were phishing and compromised credentials. In particular, the most financially damaging breach scenarios are BEC incidents (TechCentral, 2023; TechCentral, 2024; Intelligent CIO, 2024). To support these conclusions, the South African Banking Risk Information Centre (SABRIC) revealed that financial crime in 2023 totalled almost R3.3 billion, with a 45% annual increase in digital banking fraud. Unfortunately, 60% of these cyber-crimes were banking application fraud, highlighting the need for strong cybersecurity measures (SABRIC, 2024; BankservAfrica, 2024).

One of the main causes of fraud in digital banking is phishing. SABRIC (2024) reports that mobile applications, which are frequently targeted by phishing, are involved in 60% of digital banking crimes. According to Verizon (2024), human factors are involved in 68% of breaches worldwide. South Africa is seeing an increase in ransomware attacks targeting small and medium-sized businesses, as well as local governments. Ransomware is one of the biggest threats in Africa (Interpol, 2021). According to Microsoft (2024), ransomware activity has increased 2.75 times worldwide.

South African local governments have been a target to almost all cyber-threats and attacks. Local government employees use digital devices for their daily duties and personal use. The latter puts them at risk and vulnerable to cyberattacks and cyberattacks. In 2019, in the City of Johannesburg (CoJ) essential services, such as traffic signals and billing, were shut down due to a ransomware attack on the (Kharas, 2019). Since then, the City has improved cybersecurity procedures and restored its systems (Kharas, 2019). This event brought to light weaknesses in the city's cybersecurity framework and emphasised the need for extensive changes (Ntuli & Puthan, 2020). Furthermore, the Nelson Mandela Bay Local Government information technology (IT) infrastructure was breached in 2020, leading to service interruptions and possible sensitive data breaches (Nkwanyana, 2020). As a result, authorities have since implemented cybersecurity measures to counter future attacks (Nkwanyana, 2020). The Nelson Mandela Bay Local Government suffered a data breach that exposed sensitive information from citizens, prompting a nationwide conversation about the suitability of local government cybersecurity measures. The breach caused public concern about the safety of personal data and the accountability of local governments (Besson, 2022). The Drakenstein Local Government experienced a ransomware attack in 2021 that compromised confidential information and interfered with operations. The incident forced Drakenstein Local Government to shut down critical systems, leading to service delays and public outcry.

The local government response emphasised the need to immediately improve cybersecurity measures and exposed significant flaws in its incident response planning (Jansen, 2021). In this sense, South African local governments are not immune from cyber threats and cyberattacks. In this regard, South African local governments should all-encompassing:

- **Cybersecurity training and awareness strategy:** Employees should receive special cybersecurity training from local governments. To preserve data security, these programmes must emphasise threat detection, real-world scenarios, and best practices. An ongoing strategy to promote a culture of cybersecurity awareness should include regular workshops and refresher courses (Botha, 2021).
- **Investing in technological advancements:** Prioritising technology investments is imperative for local governments, with an emphasis on modern security solutions and modernising legacy systems. Frequent vulnerability assessments and audits can help identify systems that are at risk and urgently need to be upgraded (Hussein & Ndlovu, 2021).
- **Developing policies and procedures for data protection:** Creating strict data protection policies is essential. To protect sensitive data, local governments must embrace encryption technologies and consider implementing data loss prevention (DLP) solutions (Pillay & Naidoo, 2021). To reduce the chance of unwanted access, user permissions and access controls must be re-evaluated.
- **Creating response incident plans:** Local governments can be better equipped to handle cybersecurity incidents by developing and updating incident response plans on a regular basis. Officials can test their response capabilities and ensure that all employees know their roles in the event of an incident using desktop exercises and simulations (Digital Frontiers Institute, 2022).
- **Collaboration and Information Sharing:** To exchange knowledge on new threats and best practices, local governments must collaborate with other local governments and national cybersecurity organisations. The goal of programmes such as the Cybersecurity Capacity Centre for Southern Africa (C3SA) is to increase the region's ability to withstand cyberattacks (C3SA, 2021).

A complex interaction of threats and vulnerabilities characterises the cybersecurity environment facing local governments in South Africa. These can be anything from human error and technical flaws to deliberate attacks motivated by politics, money, or the interruption

of public services. Such threats have far-reaching effects that affect not only operational effectiveness, but also the legitimacy and integrity of local government.

A multifaceted strategy is needed to address these issues, including putting strong policies and frameworks in place, developing a culture of awareness of cybersecurity, and strengthening technical defences. South African local governments can strengthen their defences against cyberattacks and protect the digital infrastructure necessary for efficient service delivery and public participation by implementing the suggested mitigation techniques. Failure to address existing cybersecurity threats, risks, and vulnerabilities could lead to harmful experiences of cyberattacks. The following subsection will discuss cyberattacks and their effect on South Africa, especially at the local government level.

South African local governments face a major challenge as a result of the changing nature of cyberattacks. These attacks are becoming more frequent and sophisticated, reflecting global trends. However, they also highlight particular vulnerabilities in the South African context, such as fragmented governance, outdated infrastructure, and limited cybersecurity capacity. The opportunistic, political, or financial motivations of these attacks highlight the need for a prompt and well-coordinated response. The ramifications are extensive, impacting not only the provision of municipal services and public trust but also causing economic instability through interrupted operations, monetary losses, and harm to one's reputation. A multifaceted strategy including technical protections, legislative changes, and increased public awareness of cybersecurity is needed to combat these threats. According to this thesis, gamification presents a viable approach to improve learning and participation among municipal employees, which will ultimately increase the resistance of the South African local government to cyberattacks.

1.3 Significance of the study

Different methods are used to combat cyberattacks and cyberthreats, as well as to increase levels of cybersecurity awareness within the organisation. However, more studies continue to point to the fact that traditional methods do not work well. Therefore, game-based cybersecurity awareness has been recognised as an effective cybersecurity strategy (Nwokeji et al., 2020; Matovu et al., 2022; Prümmer, 2024; Ahmed et al., 2024). It promises to be a more effective way of reducing the lack of cybersecurity in local governments.

The significance of this study comes from the need to strengthen cybersecurity postures in the context of increasingly complex cyber threats facing local governments. Public organisations are the custodians of sensitive data and critical infrastructure; therefore, resilience to cybercrime is paramount. Improving cybersecurity awareness not only empowers employees with the knowledge to identify and respond effectively to threats but will also contribute to the security culture of local governments (Peltier, 2016). By identifying and proposing a customised gamification approach, this study aims to contribute to existing literature on effective cybersecurity awareness strategies. Therefore, we provide practical recommendations for implementing cyber security awareness using games within the South African local government.

1.4 Problem statement

As cybercriminals increasingly exploit human factors as the weakest link in security chains, there is a need for an engaging, context-appropriate, and evidence-informed approach to local government cybersecurity awareness that improves measurable competencies, particularly phishing recognition, password hygiene, and data safety, beyond what traditional training methods achieve. The researcher, who is the employee at the local government, has observed that the local governments in South Africa have struggled to implement effective strategies that keep up with evolving cyber threats (Norris et al., 2021; Pieterse, 2021; Malele and Mphasane, 2025). Moreover, the Traditional methods of cybersecurity training and awareness campaigns have often been met with apathy and disengagement from employees, resulting in inadequate understanding and readiness to defend against cyber risks (Pieterse, 2021). This disengagement could undermine the efficacy of existing cybersecurity frameworks and initiatives within local governments, therefore, exposing them to potential breaches and data loss. Subsequently, this problem hinders the local government's ability to operate effectively and maintain the highest standards of service delivery, as would be the case if these challenges were adequately addressed. (Pieterse, 2021).

This study sought to address this gap by using gamification techniques to raise awareness of cybersecurity among local government employees, thus strengthening the overall local government security framework.

1.5 Study aim and objectives

1.5.1. Study aim

The main aim of this study was to develop and make recommendations to improve cybersecurity awareness using a gamification approach for the South African local government. It encapsulated the desire not only to identify the shortcomings of existing initiatives, but also to propose effective solutions grounded in contemporary educational practices. Using gamification, the investigation sought to develop more engaging, participatory and effective recommendations for cybersecurity awareness that align with the specific needs of local government employees.

1.5.2. Study objectives

The following primary and secondary objectives were proposed to assist in achieving the main aim:

A. Primary objectives (PO)

- To improve the South African local government cybersecurity awareness strategy by making recommendations drawn from the literature and exposure to gamified cybersecurity training.

B. Secondary objectives (SO)

- The SO are further delineated into theoretical and empirical objectives: using a gamification approach.

(i). Theoretical objectives (TO)

- TO1: To explore the literature on different cybersecurity awareness strategies, frameworks, and best practices to identify key elements, design considerations, and validation methods for the development of cybersecurity awareness strategies using gamification.
- TO2: To explore the literature on the gamification tools and techniques that can be used to increase awareness of cybersecurity. Then identify and select cybersecurity

games that is suitable for the specific context of the cybersecurity awareness context.

- TO3: Consolidate the literature recommendations for cybersecurity awareness using a gamification approach.

(ii).Empirical objectives (EO)

- EO1: Conduct a brief survey using questionnaires to identify the level of awareness of local government employees.
- EO2: Develop focus groups for local government employees, allowing them to interact with the selected cybersecurity awareness game.
- EO3: Use semi-structured interviews to understand the cybersecurity awareness of local government employees to verify the recommendations formulated from the literature and the interaction with the selected gamification tool.
- EO4: Compile a final list of recommendations for cybersecurity awareness.

1.6 Study research procedure

In the early twentieth century, the Introduction, Methodology, Results and Discussion (IMRAD) was introduced as a contemporary norm and it began to standardize a decreasing use of the literary style (Sollaci and Pereira, 2004; and Oriokot et al., 2011). The IMRAD was adopted in this study, and it was implemented using the research design highlighted in Figure 1-1.

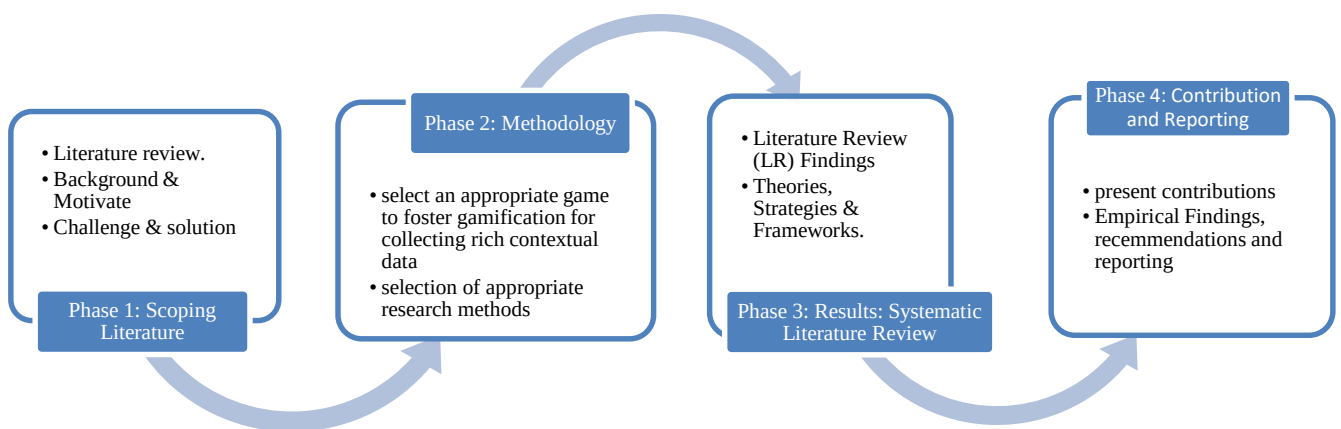


Figure 1-1: Study research procedure (Source: Author, 2024).

Figures 1-1 illustrate a four-phase research procedure that was adopted in this study. These phases are aligned with the methodological action research steps. The first phase was geared toward scoping and using the literature to develop the background, motivate, introduce the challenge of cybersecurity in local government, and motivate the need for a solution by looking at LoD-1 as the main contact point to address the challenge. Since this study adopted, IMRAD, the Phase 2 introduces the adopted methodology by focusing on the research paradigm and research design. Furthermore, it presents this study method to select the appropriate tools and conduct data collection. Phase 3 of this study focus at reporting on the systematic literature review (SLR) study to sift on key cybersecurity theories, models and framework relevant to local government, the gamification strategy relevant to be adopted in local government and raising the key threats and vulnerabilities aligned with local government. Furthermore, it provides the results, analysis, and recommendations after conducting different experiments within the action research context. The last phase, Phase 4, presents the main contribution of the study by reporting on the study findings and provide the conclusion.

1.7 Study contribution

The result of this study contributes to the existing body of knowledge on cybersecurity awareness strategies by emphasising the use of games as a training tool to improve cybersecurity usability and efficacy, and to make recommendations for cybersecurity in the local government context. Furthermore, it contributes an innovative training method that highlights the unique cybersecurity problem faced by local governments. These recommendations and methods (highlighted in Chapters 2 and the 3) and recommendation (highlighted in Chapter 6) could be used by public and private organisations to improve their cybersecurity posture.

1.8 Chapter Layout

The chapters of this dissertation are as follows:

- **Chapter 1: Introduction**

This chapter introduces the research by explaining the problem, its significance, and the objectives of this study. It includes a review of the relevant literature,

describes the research procedure, and highlights the expected contributions of the study.

- **Chapter 2: Methodology**

Here, this research approach is described in detail, including the philosophy, design, and methods used. It explains the research environment, population, and sample size, and data collection techniques and tools. Ethical considerations, along with measures to ensure validity and reliability, are also discussed.

- **Chapter 3: Findings – Scoping Literature Review**

This chapter presents an overview of cybersecurity threats, risks, and vulnerabilities. It reviews key theories, models, and frameworks, and best practices and strategies to improve cybersecurity awareness. Recommendations based on this review are provided.

- **Chapter 4: Findings – Systematic Literature Review**

The focus here is on identifying cybersecurity games suitable for awareness training. It discusses design considerations, validation methods, and gamification tools and concludes with recommendations for integrating gamification into cybersecurity strategies.

- **Chapter 5: Empirical Findings**

This chapter reports findings from focus groups and interviews. Explore themes such as knowledge and confidence in cybersecurity, learning outcomes from gamified training, and the applicability of this knowledge in real-life situations. It also examines perceptions of gamification in local government and provides recommendations based on these insights.

- **Chapter 6: Contributions**

Summarises the key contributions of the study, including recommendations for a multilayered defence approach, regulatory frameworks, third-party monitoring, and strategies for implementing gamified cybersecurity awareness in local government settings.

- **Chapter 7: Lessons Learned**

Reflects on challenges and opportunities encountered during the literature review and data collection phases, such as participant availability and willingness.

- **Chapter 8: Conclusions and Future Studies**

Restates the study objectives and explains how they were achieved. It provides a comprehensive conclusion and offers recommendations for future research, including longitudinal studies and a culturally relevant gamification design.

1.9 Conclusion

The findings of this study provide an introduction and an overview of the problem. The introduction established a foundational orientation on the need to investigate the enhancement of the cybersecurity awareness strategy within the local government of South Africa. The main objective highlighted in this chapter is the fact that a gamification approach to cybersecurity awareness could be well aligned with the empowerment of organisations, especially the local government. The critical importance of addressing cybersecurity threats in this specific context was highlighted, along with the need for more effective training methodologies that actively engage and educate.

CHAPTER 2

METHODOLOGY

2.1 Introduction

The methodology chapter is a critical component of any academic research project and outlines the philosophical foundations, research design, and data collection strategies used to achieve research objectives. The methodology provides guidelines for conducting research to ensure that the research process is systematic, consistent, and in accordance with the research questions. It also increases the credibility and reliability of the results by making the research process transparent and replicable. The methodology selected in this study is particularly important in the context of the recommendation to improve cybersecurity awareness in South Africa's local government through gamification. Cybersecurity is a complex and multifaceted issue that intersects human behaviour, organisational culture, and technological systems. Therefore, it requires a methodological approach capable of capture the depths and nuances of the experiences, perceptions, and context realities of the participants.

The Chapter begins with a discussion of the research paradigm, including the rationality of adopting a qualitative approach. Then it explains the philosophical attitude of interpretation and how it relates to the objectives of research. The Chapter also describes research strategies based on interpretation case studies and describes the methods of collecting data, including semi-structured interviews, focus groups, and literature reviews (Gill, 2008).

Finally, the Chapter presents the assessment framework for field research interpretation based on the principles of Klein and Meier (1999), which guided data analysis and interpretation. The Chapter clarifies the method of choice and its justification and sets the foundations for understanding how research is conducted and the results obtained.

2.2 Research Philosophy

Research philosophy refers to a set of beliefs and assumptions about how knowledge is developed. There are three different research paradigms: positivism, interpretivism, and pragmatism (Saunders et al., 2019). This study is grounded in interpretivist philosophy, which emphasises understanding the subjective meanings and interpretations individuals assign to their social contexts. This research philosophy is appropriate for investigating recommendations for cybersecurity awareness strategy through gamification for a South African local government entity because it allows for a thorough examination of individuals' perceptions, attitudes, and behaviours, and their interactions within the specific cultural and context of a South African local government.

Ulz (2023) supported the use of an interpretivism paradigm for research of this nature by advising that in selecting the research paradigm for the study it is imperative to consider the four pillars that support the research paradigm framework, which is ontology, epistemology, axiology, and methodology. The picture below illustrates the four pillars of research paradigms as explained by Kivunja and Kuyini (2017).



Figure 2-1: Pillars of research paradigms (Kivunja and Kuyini, 2017)

To bring these four pillars of the research paradigm into a sound dialogue with the study, we begin with ontology, a branch of philosophy that studies the existence of reality, the truth about phenomena, and whether there is one reality, multiple reality, or no reality (Ulz, 2023). In the context of the study, ontology is that local government managers, employees, and IT staff understand and experience cyber threats and are a multitude of realities about the phenomena under study. To know what the research intends to uncover and how to discover it, researchers turn to the study's epistemology.

Epistemology refers to the study of knowledge and how we can understand reality. In addition, it includes the scope and ways to obtain and validate knowledge (Abbadia, 2022). This research aims to explore the knowledge of cyber threats in local government. In addition, these realities (unknown) have been discovered by interpreting various perceptions of local government management, IT staff and employees on this topic collected through semi-structured questions. In addition, the data generated for the study were examined and verified by comparing the data of the recording tape with the data recorded by the researcher to verify the validity of the data. To check the moral value of knowledge, I then turned to axiology.

Kivunja and Kuyini (2017) observe that axiology is the ethical question of what is good or bad, what is wrong or what is right, and what researchers need to consider in planning research proposals. Furthermore, the axiology is shaped by guiding researchers to align their values with ethical principles, make ethical decisions throughout the research process, give priority to the welfare of participants, maintain the integrity of the research, and consider social responsibility (Turin, Chowdhury, and Raman, 2024). Consequently, to bring it into the context of the research, to the study's epistemology, the knowledge sought by the research and the way it must be discovered, we assume that it will not harm, mislead, fight, or violate the rights of the management of the local government, IT personnel, employees involved in the research, those who will receive the preliminary report and the final product of the research; rather, it will benefit the management of the local government, IT personnel, and employees. The last pillar is the methodology used, which describes how to find the knowledge and truth of the phenomena.

Ulz (2023) Methodology refers to how to study the environment and validate the acquired knowledge. In addition, it seeks to answer questions about how to discover reality. As regards

the methods used to discover existing realities in this research, the researcher considers semi-structured interviews and document review to be suitable for using data generation methods for selected case study designs because they help the researcher to investigate phenomena appropriately. However, these pillars are connected in that epistemology provides knowledge, ontology checks whether there is knowledge, axiology checks whether it is wrong or right, and moral value checks if it exists.

2.3 Research Design

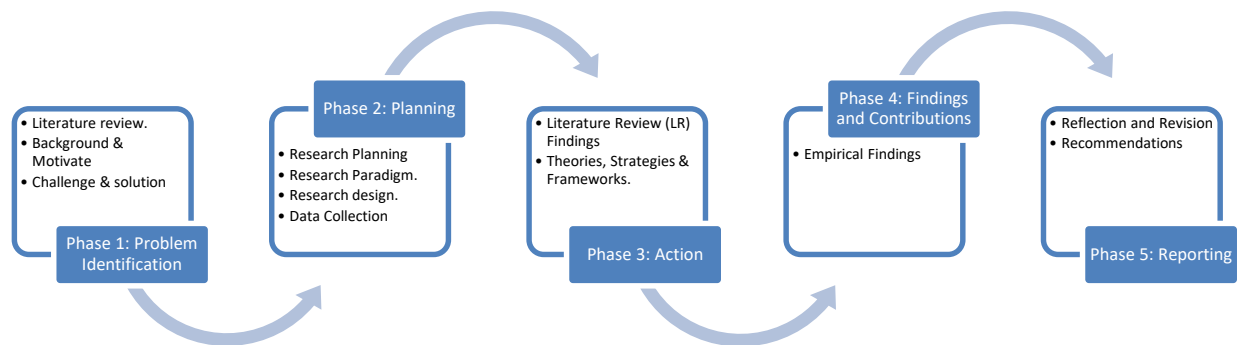


Figure 2-2: The adopted research process (Source: Author).

A case study approach was used to facilitate a holistic investigation (Chetty, 2013). Case studies are effective in analysing real-life events and their contextual relationships. Figures 2-1 illustrate a five -phase research procedure that was adopted in this study. It follows the action research steps (Mertler, 2021; Sithaldeen, 2024), namely:

- (i) **Phase 1: Problem Identification** – starting point of this study in which literature review using either narrative or scoping literature techniques was conducted to ideate and clearly sift the problem in the study area. It was also used to develop study background, motivation, significance, aims and objectives. The results of this step are captured in Chapter 1 of this dissertation.
- (ii) **Phase 2: Planning** – in this phase, the research strategy or research methodology aimed at addressing the identified problem and how the study will be conducted was adopted. The results of this step are captured in this chapter, which is Chapter 2.
- (iii) **Phase 3: Action** – the planned strategies are then implemented in this stage. In this study both systematic literature review and empirical research will be conducted. Some research databases identified in Phase 2 and recruitment strategy for

participants are put into action. The results of this step are captured in Chapter 3 of this dissertation.

- (iv) **Phase 4: *Findings and Contributions*** – the outcomes of the action implemented in Phase 3 are observed and analysed to draw conclusions about their effectiveness and identify areas for improvement. This stage ensures that the research remains grounded in the real-world context. Furthermore, based on the insights from these findings, then the action phase will either be repeated, or the recommendations in a form of a contribution are made. The latter initiates the next phase. The results of this step are captured in Chapter 4 of this dissertation.
- (v) **Phase 5: *Reporting*** – the entire study outcomes, recommendations and contributions are summarised and reported through this dissertation as a conclusion. The results of this step are captured in Chapter 5 of this dissertation.

2.4 Research Methods

Different questions and problems can be tackled by different methods, which means that a researcher must make a choice on which method they are using and also reflect on why that method is the most viable method to use. This choice requires some consideration of what the ideal approach is and what is practically achievable. Both the ethical assessment and the methods the researcher can perform are important for method choices, and what is economically and time-wise realisable (Bhandari, 2023). When the research is complete, the researcher must again discuss the method, which involves self-criticism; the researcher should then consider how the chosen method worked and whether the choice of the method was good enough to arrive at a good answer to the research question (Bhandari, 2023). There are generally three research methods that a researcher could choose from:

- (i) **Quantitative method** – starts with a research question that indicating a problem statement and possible way of collecting data (Bhandari, 2023). It provides data in the form of measurable mechanism. Some of the most common characteristics of quantitative research is that it is systematic, which means that surveys are given with fixed answers, data collection is done without direct contact with the field being studied, and the presentation of findings aims to provide explanations, also by using quantitative

research method, the researcher looks at the phenomena from the ‘outside’ and strives to be neutral in his research as much as possible (Bhandari, 2023).

- (ii) **Qualitative method** – aims to capture opinions and experiences that cannot be expressed by numbers or measurements (Bhandari, 2023). It comprises close contact between the researcher and people in the field through participatory observation and/or interviews (Thagaard, 2018). The common characteristics of qualitative research are the in-depth and an effort to present a lot of information from a small survey unit (Thagaard, 2018; Bhandari, 2023). This method is also flexible, as the interviews done are characterised by flexibility without fixed answers; by doing so, the qualitative method tends to be much closer to the field being studied, unlike the quantitative method (Bhandari, 2023).
- (iii) **Mixed method** – it’s a method that combines quantitative and qualitative data collection (Ngulube, 2022). It enables triangulation, which is the use of various ways when collecting data. Mixed approaches reduce errors since the different methods correct each other (Thagaard, 2018; Ngulube, 2022; Bhandari, 2023).

In this study, the mixed method research approach was adopted to make recommendations that will improve a gamified cybersecurity strategy for the local government of South Africa. Data were collected from both primary and secondary sources. The data collection technique included literature review, questionnaires, semi-structured interviews, and focus discussion groups (Gill et al., 2008).

2.5 Research Environment

The public sector in South Africa is divided into three government levels: (i) the national, (ii) provincial, and (iii) local governments. The local government is subdivided into three categories:

- Category A is the metropolitan municipalities governing big cities,
- Category B is the local municipalities governing towns and surrounding rural areas, and
- Category C is the district municipalities governed through the coordination several local municipalities in a region.

South Africa comprises 9 provinces made up of 257 number of municipalities (8 metropolitans, 205 local municipalities and 44 district municipalities). In total Limpopo local government comprises 27 municipalities (5 district municipalities and 22 local municipalities) as illustrated in Figure 4-1. This study was conducted at the Collins Chabane Local Municipality (CCLM).

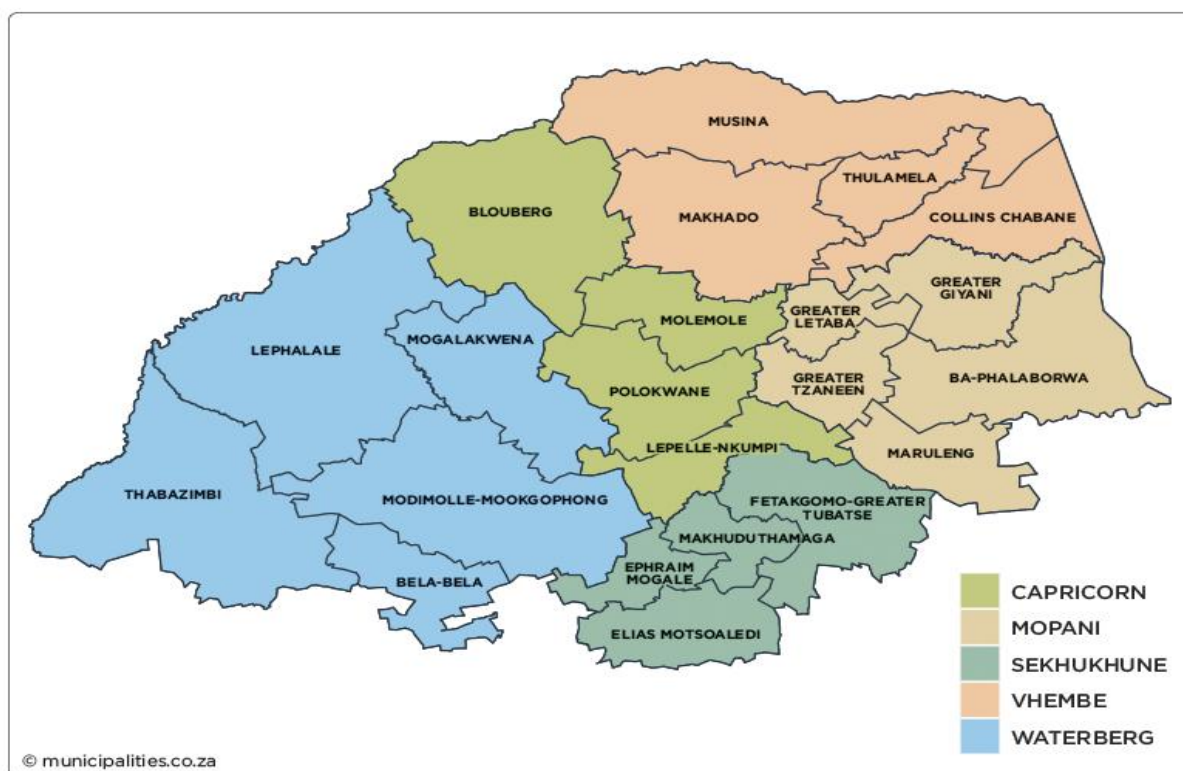


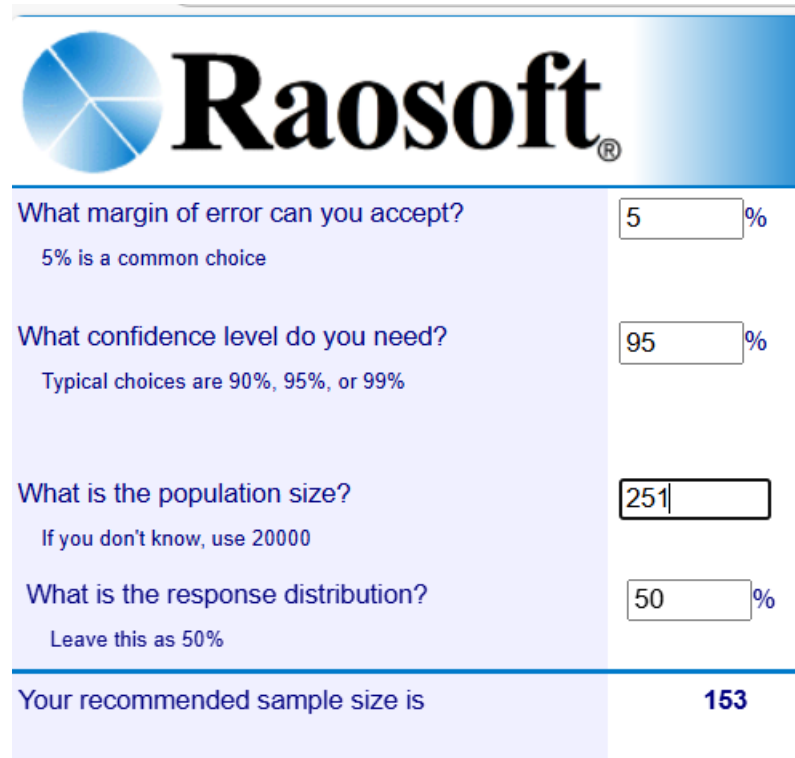
Figure 2-3: Map of Limpopo Province (Source: Municipalities of South Africa).

The CCLM is one of Limpopo Province Municipality and is situated in the Vhembe District Municipality approximately 191km north of Polokwane City the capital of the Limpopo Province, South Africa. The municipal land area covers 5 467.216km² (22° 35' S 30° 40' E) in extent with a population of approximate of 347 974 inhabitants. Apart from the two main towns namely, Malamulele and Vuwani Town and 173 Villages, the municipal area also includes 3 informal settlements.

2.6 Population and Sample size

The target population refers to the population wherein a sample will be drawn and in a case study approach (such as the one reported in this dissertation) the researchers needs to have access to this population (Gross et al., 2018; Ackerman et al., 2019; Bell, et al., 2019; Casteel and Bridier, 2021). The researcher must have access to this population of interest during the

interview process. It is important to describe the target population to ensure inclusivity properly and obtaining sufficient data; while at the same time guarding against including people who may not add any value to the phenomenon in question (Gross et al., 2018). Furthermore, boundaries of the target population must be clearly defined to avoid misunderstanding which lead to poor resources management (Ackerman et al., 2019).



Question	Answer
What margin of error can you accept? 5% is a common choice	5%
What confidence level do you need? Typical choices are 90%, 95%, or 99%	95%
What is the population size? If you don't know, use 20000	251
What is the response distribution? Leave this as 50%	50%
Your recommended sample size is	153

Figure 2-4: The adopted research process (Source: Author).

In this regard, the CCLM comprises a population of 251 employees (20 managerial members, 62 ICT staff members, and 169 other staff members). In the cybersecurity context all employees comprise the CCLM first line -of-defence (LoD) since they all come into interaction with the digital or online systems making them cyber-vulnerable individuals. To draw a representative sample from CCLM, the Raosoft sample calculator was used as illustrated in Figure 2-3. In this regard, 153 random sample was selected to participate in this study.

2.7 Data Collection

Data collection is gathering of information that may be utilised for analysis or study, including facts, figures, and observations (Bairagi and Munot (2019). There two sorts of information that may be obtained in data collection: (i) primary data and (ii) secondary data. To get a deeper understanding of a topic, researchers create primary data by performing their surveys, interviews, and experiments; in contrast, secondary data have already been collected for record-keeping purposes by large government bodies and agencies (Narkhede, 2020). In this study, systematic literature review was used to collected the secondary data, while questionnaires and interviews were used to collect the primary data.

2.7.1. Scoping and Systematic literature review

The literature review (LR) approaches (scoping and systematic) were adopted in this study. The scoping literature review (ScLR) was used to explore the literature on different cybersecurity awareness strategies, frameworks and best practices relevant to local government. While the systematic literature review (SLR) was used to identify key elements, design considerations and validation methods for developing cybersecurity awareness strategies using gamification in a local government setting. In this regard, the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines to ensure that the choice and collection of relevant documents are clear, repeatable, and complete were consulted and the PRISMA framework was used (Moher et al., 2009). To develop the PRISMA flow diagram (see Figure 2.1) the following research protocol was followed:

A. *Problem Identification*

The review was conducted using the following research questions as the basis of investigation:

- What cybersecurity strategies, frameworks, and best standards are used to improve cybersecurity awareness? How are these strategies, frameworks, and best standards validated in practice?
- What design principles support effective gamified learning?
- Are there any cybersecurity awareness strategies using gamification in a local government setting?

B. Identification of research databases

The following information or research sources or portal or databases were identified using narrative literature review and were consulted:

- ACM Digital Library,
- Education Resources Information Centre (ERIC),
- Google Scholar,
- IEEEExplore, and
- Scopus.

Furthermore, the government resources cybersecurity related sources were consulted (i.e. SA Cybersecurity Hub, SA DoJ&CD Cyber Safety, USA Center for Development of Security Excellence (CDSE) - Cybersecurity Trivia Twirl, WeForum).

C. Search Protocol

(i) Search strategy:

A search strategy using focus on cybersecurity awareness through gamification using the following keywords: cybersecurity games, cybersecurity trivia twirl, cybersecurity awareness, serious games, cybersecurity training, cybersecurity awareness education and training cybersecurity framework. The following Boolean operations were used:

- Cybersecurity AND Awareness AND (Framework OR Strategy OR Model OR Best Practices) AND (Education AND Training) AND (Local Government OR Municipality);
- Cybersecurity AND Awareness AND (Gamification OR Serious Games OR Game-based learning) AND (Local Government OR Municipality);
- Cybersecurity AND Awareness AND (Gamification OR Game-based learning OR Serious Games) AND (Framework OR Strategy OR Model OR Best Practices) AND (Local Government OR Municipality).

(ii) Eligibility Criteria

The following inclusion and exclusion criteria were used to determine which studies were eligible:

- Inclusion Criteria
 - Peer-reviewed publication: (a) journal articles, (b) conference papers, and (c) official reports.
 - Published between 2015 to 2025.
 - Written in English.
- Exclusion Criteria
 - Gray Literature comprises non-peer-reviewed sources (e.g., blogs, opinion pieces, etc.).
 - Studies that do not involve keywords:
 - cybersecurity awareness
 - Gamification, Serious games or game-based learning.
 - Framework OR Strategy OR Model OR Best Practices
 - Not written in English

D. Screening and Data extraction

The initial search for retrieving the articles from databases yielded an output of 312 records which seemed appropriate for this study. Using a duplication filter, 87 articles were removed leading to 225. A further screening of the articles using no title alignment and grey literature filter as screening method led to a total of 90 articles being removed which led to the remaining 135 articles being filtered for title and abstract alignment to keywords led to removal of further 48 articles. In this regard, a total of a total of 87 articles remained, of which the further screening using direct keywords that could lead to a strategy (i.e. cybersecurity awareness framework or strategy using gamification in local government setting), led to a total of 25 articles remaining for analysis. The entire process discussed in the latter paragraph is illustrated by a PRISMA flow diagram in Figure 2-5.

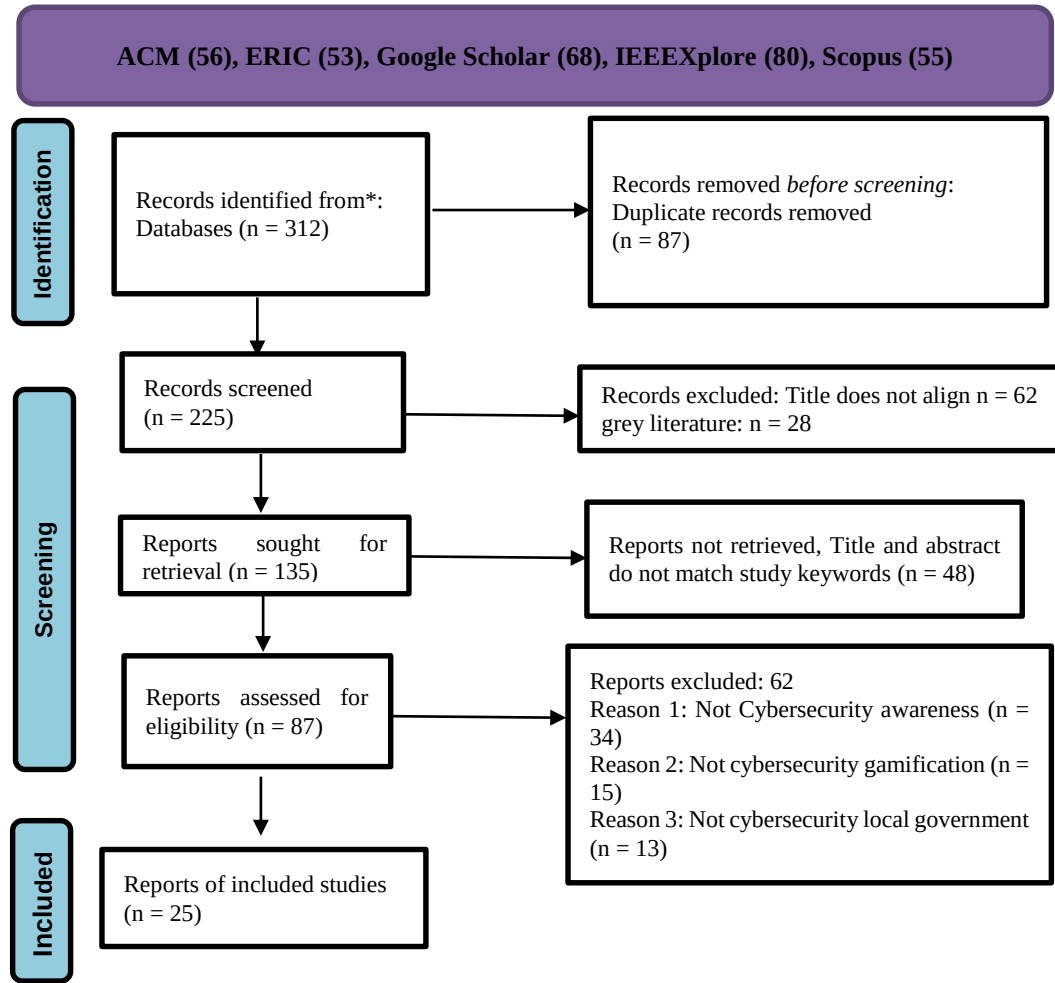


Figure 2-5: PRISMA flow diagram (Source: Author)

2.7.2. Empirical data collection techniques

This study adopted a case study approach in which it collected primary data using questionnaires, focus group discussion and interviews.

A. Questionnaire

In the context of this study, the questionnaire was used to ascertain the local government employees as the LoD-1 cybersecurity awareness education, understanding and willingness to participate in the cybersecurity awareness training. In this regard, an online announcement alerting the employees regarding the cybersecurity awareness brief survey was distributed through e-mails to all CCLM employees. This announcement had a link to distribute the questionnaire using a google form. The employees were given right to opt-out of the survey at any time. The questionnaire did

not collect their identity and the google form was returned automatically without linking by showing their e-mail addresses since the questionnaire was anonymous. The aim was to collect data from at least 153 participants as illustrated by Raosoft (see Figure 2-3).

B. Focus group

After need analysis was conducted as illustrated in par. The CCLM employees were scheduled to attend in-house cybersecurity training using strategic workshops. During the workshops, different focus groups were formulated using a random selection of 10 people per group, amounting to a total of 25 groups for the entire CCLM. The group had to select their group names, i.e. cyber-defenders, with that name being given to each group member. The latter made group members anonymous.

C. Interviews

A delphi procedure is a structured, iterative forecasting method that relies on a panel of experts to reach a group consensus (de Villiers et al., 2005). In this regard, 10 %, amount to 25 people were selected for the interview. This cohort was made up of the employees (mainly executive, senior and middle managers).

2.8 Research Tools

The google forms were used for collecting the data through questionnaire. They also assisted with the data analysis through its dashboard. Furthermore, the NVivo and Microsoft Excel were used to analyse the collected data. An audit trail has been maintained to record decisions, interpretations and methodological adjustments, which improves the reliability of the findings.

Beyond the questionnaires and interview questions, the other research tool that was used in this study was a cybersecurity game, a concept known as cybersecurity gamification. Gamification has been successfully applied to deliver important outcomes in other disciplines and can also be used to deliver cybersecurity awareness.

Cybersecurity Trivia Twirl

SPIN THE WHEEL

PAUSE

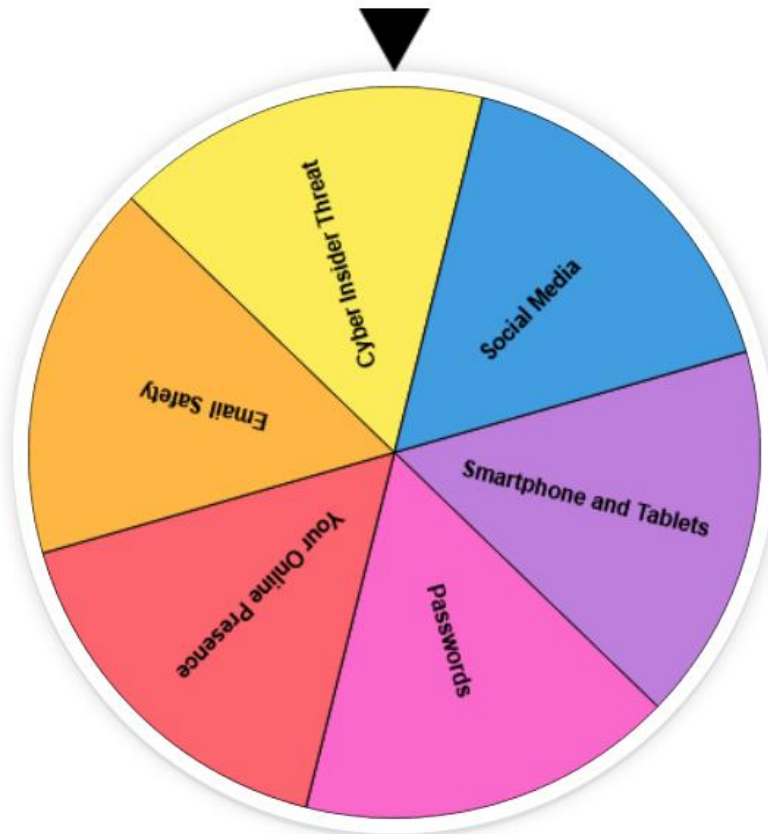


Figure 2-6: CDSE Cyber Trivia Twirl (Source: CDSE)

A pre-analysis of available cyber-security games using scoping literature review (ScLR). In this regard, the Center for Development of Security Excellence (CDSE), which is the custodian of different cybersecurity games, was consulted. Due to its wheel structure that has six segments (Email Safety, Cyber Insider Threat, Password, Smartphone and Tablets, Social Media, and Your online presents), each representing a different Cybersecurity category, Cyber-Trivia Twirl (see Figure 2-6) was selected and randomly tested for the suitability in the municipality context by two CCLM IT employees prior to its usage in this study.

You've landed on Cyber Insider Threat.

TAKE THE QUIZ!

Which of these should be considered a cyber insider threat?

SOMEONE WHO
INTENTIONALLY RELEASES
TOP SECRET INFORMATION
VIA COMPUTER OR OTHER
ELECTRONIC MEANS

SOMEONE WHO
ACCIDENTALLY DISCLOSES
PROTECTED INFORMATION
BY STORING IT IN THE
"CLOUD"

SOMEONE WHO COPIES
PROTECTED INFORMATION
TO A FLASH DRIVE AND
GIVES IT TO THE PRESS

ALL OF THE ABOVE



Figure 2-7: CDSE Cyber Trivia Twirl Quiz (Source: CDSE)

Figure 2-7 illustrates the CDSE's Cyber-Trivia Twirl. It is known as the cybersecurity SPIN THE WHEEL button game (see Figure 2-5) because it allows the player to spin the wheel until it stops in one of the segments which provide at least five multiple choice questions. The player will then answer the questions. If the player correctly answers three or more questions, that category segment is removed from the wheel and the player may spin the wheel again to play in other segments. If the player incorrectly answers three or more questions, the player is provided a chance to try again or spin the wheel to select another category. Play continues until all six categories have been completed successfully.

2.9 Ethical Protocol

Tracy (2024) defines research field work experience as hands-on practical participation in a specific research project or study that takes place outside of a laboratory or controlled environment. This is also mentioned by Howlett (2022), who defines fieldwork as a type of inquiry in which researchers enter a new context, a field site, or sites, to conduct their investigation. As a result, the fieldwork for this study was carried out in the CCLM by the researcher who was an Information Technology manager of CCLM.

Before starting any data collection activities in the local government, the researcher submitted a letter requesting permission, along with the ethical certificate obtained from university. This was a very important formal procedure to obtain assistance from the Municipal Manager (executive responsible for the municipality). In this regard, all members of the local government were briefed. The researcher first scheduled an appointment with the Municipal Manager and his senior managers during the senior management meeting, to discuss the research topic, who the participants are and how they will be selected, ethical considerations, and other research logistics. In this regard, all the necessary ethical protocols were followed and permission for this study was granted (see Appendix).

2.10 Validity and reliability

To ensure validity, this study used methodological triangulations, looked for patterns in responses provided through questionnaires, focus group discussion, interviews, and observations. The latter also provided data collection and analysis reliability.

2.11 Conclusion

In this chapter, the research design and research philosophy are presented. In this study, the concept of a focus group was presented since the research was conducted at the CCLM which is an employer of the researcher. In this regard, all ethical clearance processes were presented. The research design was conducted adequately to achieve all the objectives.

CHAPTER 3

FINDINGS: SCOPING LITERATURE REVIEW

3.1 Introduction

The aim of this Chapter is to present the work conducted to achieve TO 1:

“TO1a: To explore the literature on different cybersecurity awareness strategies, frameworks, and best practices to identify key elements...”

There are at least five literature review techniques (Munn et al., 2018; Snyder, 2019), namely: (i) Narrative literature review, (ii) Systematic literature review, (iii) Integrative review, (iv) Meta-analysis Bibliometric analysis, (v) Critical thinking review and (vi) Scoping review. The general purpose for conducting scoping reviews is to identify and map available evidence about the concept to your topic of discussion (Munn et al., 2018).

In this chapter, a scoping literature review methodology was used to structure the literature review related to this study. This was guided by the question: What are different cybersecurity awareness strategies and cybersecurity games that relevant and necessary for developing cybersecurity awareness strategy using gamification? In this regard, this Chapter begins by discussing the different cybersecurity threats and attacks, then looks at the types, frameworks, strategies or mitigating against the threats and attacks, and then discuss the risks and vulnerabilities of not dealing with the threats and vulnerabilities.

3.2 Cybersecurity threats and attacks

The threat to cybersecurity can have a profound impact on individuals and organisations. For example, the consequences in industry could include (i) monetary losses caused by cyberattacks, including the cost of cleaning up, legal fees, and damage to customers' reputations; (ii) data breaches can reveal private information, lead to identity theft, and privacy breaches, which can lead to penalties; (iii) operating disruptions can disrupt business operations, lead to lost productivity, and time lost (IBM, 2021); (iv) lastly, reputation damage can lead to a decline in market share and a decrease in customer trust (PWC, 2023).

Cybersecurity threats are any events or actors that could take advantage of weaknesses in information systems and harm resources, businesses, or people (NIST, 2011). This definition used within the ISO/IEC 27005 framework, serves as the foundation for cybersecurity risk management (ISO, 2018). It helps to define and categorise threat actors based on their strategies and motivations. For proper categorisations, see Table 3-1 below.

Table 3-1: Summary of possible types of actors, strategies and motivation used in cybercrimes

Threat Actors	Strategy/Technique	Motivation
Cyber-criminals	• Phishing • Ransomware	Money
National-state actors	• malware including ransomware, Trojan horses, and viruses	Espionage and/or sabotage
Hackers/Attackers	• cyberattacks ○ Phishing, ○ Distributed denial-of-service (DDoS) ○ Man-in-the-middle ○ Password attacks. ○ Social engineering ○ Code injection	Political, economic and/or Ideological
Employers, employees, subcontractors or service providers.	• Negligence • Lack of awareness • Business email compromise (BEC)	Misuse of position and power Money

As illustrated in Table 3-1, here are different motivations behind cybersecurity threats or cyber-crime threats. For example: (NCSC, 2023; Arroyabe, 2024; Abdullah et al., 2025):

- (i) many cybercriminals or cyber-threat actors are motivated by financial gain, whether through ransomware extortion, direct theft, or the sale of stolen data on the dark Web;
- (ii) political or ideological advantage, and hacktivist groups use cyberattacks to achieve their political or social goals, usually against organisations that disagree with them;
- (iii) corporate espionage obtains trade secrets, intellectual property, or private information, rival organisations can launch cyberattacks; and
- (iv) nation-state activities carry out espionage or sabotage against other countries, vital infrastructure, or entities, governments are increasingly using cyberwarfare.

At first lens, the cyber-threat actors will always target vulnerable or penetrable loops of any individual or organisational system. Cyber-threat actors or cyber-attackers or Hacktivist or

Hackers will try to penetrate a cyber-ecosystem using the LoD-1 which is the human being carrying the device to be cyberattacked (i.e. cyber penetrated) (Al-Mohammed and Baydoun, 2024). For example, human factors are involved in 68% of breaches worldwide (Henrico and Els, 2025). To achieve the cyber-attack of cyber-penetration different methods are used as discussed below.

3.2.1. Phishing attacks

Phishing is a type of cyberattack in which attackers pose as trustworthy organisations, such as banks, government agencies, or service providers, to trick victims into releasing private information such as access cards, bank account information, or personal identification numbers (Alkhalil et al., 2021). These attacks typically take the form of voice calls, short message service (SMS), or emails and frequently contain malicious attachments or links that install malware and lead users to phoney websites (Wan Heerden et al., 2016; Alkhalil et al., 2021). Phishing is categorised as a social engineering attack that takes advantage of people's trust instead of technological flaws. It continues to be one of the most popular and successful cyberattack techniques worldwide due to its ease of use and potency.

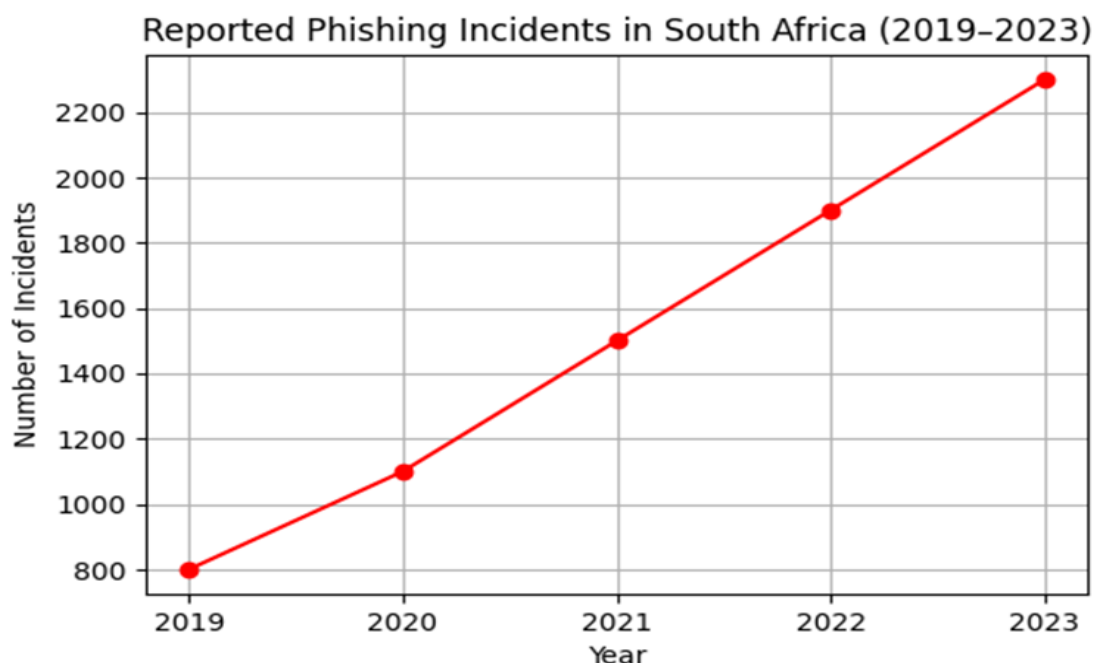


Figure 3-1: Reported phishing incidents in South Africa over five years (SABRIC, 2024).

Figure 3-1 illustrates that phishing incidents have been on the rise in South Africa since 2019. Phishing in South Africa targeted local governments, which frequently lack a robust cybersecurity infrastructure. The main source of digital banking fraud, according to SABRIC (2024), was phishing, with many attacks involving officials or vendors using hacked municipal email systems.

South African local governments have been vulnerable to phishing attacks due to older systems, a lack of cybersecurity training for staff, a heavy reliance on email for service delivery and purchases, and inadequate email authentication procedures. In this regard, phishing caused financial losses, operational issues, data breaches, reputational damage, and legal risks. The latter hinders the local government resources and propagates the erosion of public confidence.

To effectively counteract phishing attacks, local governments should incorporate multifactor authentication (MFA), email authentication protocols (SPFs, DKIMs, and DMARCs), regular trainings and simulations, central incident response plans, secure procurement procedures, and collaboration with national cyber security organisations such as SABRIC and CSIRT.

3.2.2. Business Email Compromise (BEC)

A sophisticated type of cyberattack known as business email compromise (BEC) occurs when threat actors pose as trusted individuals, such as managers, suppliers or service providers, and coerce staff members into sending money or private data (van der Merwe, 2023). BEC is extremely targeted and frequently necessitates prior investigation of victim organisations, in contrast to phishing, which spreads a wide net. BEC attacks typically use human error, urgency-based manipulation, inadequate email authentication protocols, and a lack of financial transaction verification processes. Because these attacks frequently compromise authentic accounts or are carried out in a fake email domain, detection is challenging.

In addition, BEC is among the top five cyber threats affecting the continent, according to Interpol's African Cyber Threat Assessment (2021). Due to their frequent financial transactions, procurement activities, and often immature cybersecurity, local governments make attractive targets. BEC incidents have increased in South Africa, especially in the local government. For example, according to a 2024 SABRIC report, local governments are

increasingly falling prey to fraudulent payment redirection schemes, leading to a loss of R3.3 billion in financial crime losses.

3.2.3. Denial of Service (DoS) and Distributed DoS (DDoS)

Cyber threats known as denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks are designed to overwhelm traffic systems and eliminate the availability of digital services (Osanaiye et al., 2016). DDoS attacks are more difficult to stop because they are launched from several compromised systems, whereas DoS attacks come from a single source (Pieterse, 2021).

The DDoS attacks are now common in South Africa. According to NETSCOUT's Threat Intelligence Report, in the first half of 2024, South Africa saw more than 230,000 DDoS attacks using 28 different vectors (Abu-Mahfouz et al., 2023). These vectors, which eschew conventional mitigation strategies, include TCP ACK, DNS amplification, and TCP SYN/ACK amplification. South Africa's increasing level of digital maturity (with respect to computer-related services, insurance, local governments and state portals, and telecommunications) puts it in a pivotal position in the continent's online ecosystem; thereby making a potential ground for DDos attacks (Mabunda, 2021). Furthermore, due to financial limitations and lack of cybersecurity infrastructure, South African local governments are especially at risk (Mabunda, 2021; Pieterse, 2021; Mpuru & Kgoale, 2025). For example, the South African City of Johannesburg Municipality experienced two significant cyber events in 2019: Shadow Kill hackers' network disruptions and ransomware attacks on the city's electricity supply.

DDoS attacks have several negative effects on local governments, such as financial losses from outages and recovery expenses, reputational harm and a decline in public trust, service failures that impact citizen-facing platforms, and legal risks related to data protection and governance (Letseka, 2022). The Cybercrime Act (2020), which criminalises a variety of cybercrimes and creates investigative and prosecution procedures, is part of South Africa's changing legal response to cyberthreats. But there are still legal issues and enforcement gaps, particularly when it comes to fighting transnational threats (Mpuru & Kgoale, 2025). Concern over a state's ability to regulate its digital infrastructure, or internet sovereignty, is growing. Although there are steps to strengthen national cybersecurity in the National Cyber Security Policy Framework, its execution has been uneven (Mabunda, 2021).

3.2.4. Man-in-the-Middle (MitM) Attacks

Man-in-the-Middle (MitM) attacks are cyberattacks in which malevolent actors secretly intercept and possibly change communication between two parties. These attacks steal confidential information and insert malicious content using insecure networks, weak encryption, or compromised devices (Conti et al., 2016; Marakalala & Madzivhandila, 2025).

MitM attacks were also noted as a growing concern by the INTERPOL 2024 African Cyberthreat Assessment, particularly in areas with developing digital infrastructure (INTERPOL, 2024). South African local governments are susceptible to MitM attacks due to their outdated infrastructure, insecure public Wi-Fi networks, and failure to encrypt internal communications; these attacks could result in financial transactions, unauthorised access to citizen data, and interruptions of public services (CSIR, 2024). In one instance, hackers altered banking information, redirected payments, and intercepted communications between suppliers and local government procurement offices. Implementing encryption standards in public sector systems and protecting communication channels are crucial, according to the National Cybersecurity Policy Framework (State Security Agency, 2015).

Again, the virtual private network (VPN) is network that comprises a technology that creates a secure and encrypted connection using public network to connect remote sites and users together (Hussain, 2022; Li et al., 2025; Qollakaj et al., 2025). There exist two main VPN types (Qollakaj et al., 2025): (i) Remote Access VPN – allowing anyone to join a closed network and access all services and resources from a remote location regardless of geographic location; and (ii) Site-to-Site VPN – allows the organisations with several offices in different offices to connect to the network at a hub or central office. Since, MitM uses techniques of eavesdropping to attack the target, then the VPN can help in addressing MitM attacks because it easily deals with DDoS and eavesdropping (Hussain, 2022).

These days, most employees work remotely, and local governments clients connect to government services remotely. In this regard, local governments should use secure VPNs for remote access, end-to-end encryption for all communications, frequent software and firmware

updates, cybersecurity training for employees, and monitoring of network traffic for anomalies and unauthorised access to reduce MitM risks.

3.2.5. SQL Injection

SQL injection (SQLi) is a type of cyber-attack that inserts malicious SQL code into the input field of a web application to manipulate the database (Alenezi et al., 2021). This allows attackers to access sensitive data, modify or delete records, bypass authentication, and perform database management operations (Kathayat, 2024).

South African local governments are increasingly exposed to SQLi attacks due to outdated systems, poor encryption practices, and limited cybersecurity budgets. According to a CSIR national cybersecurity survey, 55% of organisations reported application layer attacks, including SQL injections (Ngejane, 2024). These attacks often result in data breaches involving identifiable personal information (PII), service interruptions on portals used for billing, licencing, and procurement, financial losses due to fraud and recovery costs, and reputational damage. For example, South African Weather Services were shut down due to a cyber-attack that affected aircraft and maritime forecasts. Although the exact method was not disclosed, such events often include vulnerabilities such as SQLi in public-facing systems (ADF, 2025).

South African government institutions face 3,480 cyberattacks a week, SQLi being one of the most persistent threats. The National Cybersecurity Framework was accelerated to address these risks, but implementation remained uneven (Hardie, 2025; ADF, 2025). Global agencies such as CISA and FBI have issued warnings urging software developers to remove SQLi vulnerabilities and calling them "inadmissible" for their preventability (CISA & FBI 2024). These alerts emphasise the use of parameterised queries, input validation and sanitisation, Web Application Firewall (WAF), regular security audits, and penetration tests.

To protect against SQLi attacks, South African local governments should adopt secure coding practices, train developers on SQLi prevention, implement WAFs to filter malicious traffic, conduct regular vulnerability assessments, use multifactor authentication and low-privilege access control, and cooperate with national organisations such as CSIRT and CSIR to develop threat intelligence and response planning. SQL injection attacks pose a serious threat to local governments in South Africa, exploitation of weak application security, and outdated

infrastructure. As cyberattacks targeting public institutions increase, local governments must prioritise secure software development, proactive monitoring, and national cooperation to protect critical services and citizen data.

3.2.6. Zero-Day Exploits

Cyberattacks known as "zero-day exploits" target undiscovered flaws in hardware and software systems. These vulnerabilities are especially dangerous because they are exploited before the developer can release patches (Negro de Andrade et al., 2025; Bilge and Dumitraş, 2012). Due to inadequate cybersecurity funding, obsolete infrastructure, and a lack of qualified staff, South African local governments are increasingly susceptible to zero-day exploits. The State Treasury and local governments in South Africa were harmed by a recent attack that exploited a zero-day vulnerability in Microsoft's SharePoint server (Dutta, 2025). These attacks may result in long-term damage to one's reputation, disruption of public services, and unauthorised access to private information. Ransomware attacks that involve undiscovered vulnerabilities have previously affected Johannesburg and the Department of Justice (Peyper, 2024).

The critical gaps in the public sector response and readiness are highlighted in the CSIR National Survey (CSIR, 2024). The increasing threat of sophisticated cyberattacks, including zero-day attacks, throughout the continent is also highlighted in INTERPOL's African Cyber Threat Assessment Report (INTERPOL, 2024).

Proactive threat detection systems, endpoint protection, frequent vulnerability assessments and penetration tests, incident response plans, cyber security awareness programmes, and cooperation with national organisations such as CSIRT and CSIR for information sharing and coordinated defence are all ways local governments can reduce the risk of zero-day attacks.

3.2.7. Credential Stuffing

Credential stuffing is a type of cyberattack that allows attackers to access user accounts of other systems without unauthorised access using stolen usernames and passwords from previous data breaches. This is because many users reuse the same credentials on multiple platforms (Kaspersky, 2024; Abduhari, 2025).

The South African local government is increasingly vulnerable to identity theft due to outdated systems, a lack of multifactor authentication, and limited awareness of cybersecurity. According to NEC XON, more than 10,000 compromised South African credentials were discovered on the dark web, many of which were related to public domains (NEC XON, 2025). These attacks can lead to unauthorised access to sensitive local government data, disruption of services, and financial losses. The violation by the CIPC is a remarkable example of the misuse of stolen credentials to access and sell dark web data (Da Vinci Forensics, 2025). The CSIR's national cybersecurity survey showed a lack of preparedness in public institutions, many of which failed to implement basic security measures such as multifactor authentication (CSIR, 2024). The African Cyberthreat Assessment Report of INTERPOL also warns of the growing threat of credential stuffing-based attacks throughout the continent (INTERPOL, 2024).

To mitigate the risks of credential stuffing, local governments must apply multifactor authentication in all systems, regularly audit passwords and enforce strong password policies, control compromised credentials using threat intelligence tools, provide staff with cybersecurity training, and cooperate with national cybersecurity bodies for coordinated defence.

3.2.8. Social Engineering

A type of cyberattack known as "social engineering" coerces people into divulging private information or compromising security. These attacks are especially challenging to identify and stop because they rely on human psychology rather than technological flaws (Hadnagy, 2018; Hoseini & Majidi Gahrodi, 2023). Due to a lack of cybersecurity awareness and training, social engineering attacks are increasingly targeting South African local governments. Attackers frequently trick employees into divulging login information or transferring money posing as reliable authorities or service providers. Public sector organisations cited phishing and impersonation as two of the biggest threats in the CSIR 2024 cybersecurity survey (CSIR, 2024). One prominent example of this is the Business Email Compromise (BEC) scam, which used social engineering techniques to mimic suppliers and redirect payments, defrauding Buffalo City Municipality of more than R4 million (Pieterse, 2021).

The South African government is aware of the increasing danger posed by social engineering. To reduce the risks associated with human factors, the National Cybersecurity Policy Framework emphasises the need for public sector training and awareness initiatives (State Security Agency, 2015). Social engineering was also identified as a key tactic used by cybercriminals throughout the continent in the African Cyber Threat Assessment of INTERPOL 2024.

3.2.9. Supply Chain Attacks

Supply chain cyberattacks occur when threat actors breach third-party suppliers and service providers of the organisation (Martnez & Durán, 2021). These attacks indirectly compromise systems through the interconnection of contemporary supply chains (Boyson, 2014).

South African local governments are highly dependent on outside vendors for infrastructure, procurement, and IT services. Their susceptibility to supply chain attacks was enhanced by this dependence. A notable illustration of how supply chain vulnerabilities can impact local and national logistics is the Transnet ransomware incident, which caused port operations to be disrupted (Peyper, 2024). Third-party relationships were found to be the primary cause of cyber incidents in the public sector by the CSIR 2024 cybersecurity survey, which also highlighted the urgent need to improve vendor risk management (CSIR, 2024).

The coordination of cybersecurity governance, including supply chain risk assessment, is highlighted in the National Cybersecurity Policy Framework (State Security Agency, 2015). Attacks on software vendors and service providers are on the rise, according to INTERPOL's 2024 African Cyber Threat Assessment (INTERPOL, 2024).

3.2.10. Recommendations

South African local governments face a rapidly changing and serious cybersecurity threat landscape, including malware, phishing, denial of service attacks, insider threats, APTs, and IoT vulnerabilities. These attacks can have disastrous effects, including monetary losses, business interruptions, damage to one's reputation, and legal implications. Basic technologies that include the protection of computer networks should be adopted. The technologies should implement a strong security measure such as intrusion detection systems, firewalls, and

encryption protocols frequent patching and software updates to keep systems and software up to date reduce vulnerabilities exploited by hackers (Admass et al., 2024). To respond to cybersecurity threats, a comprehensive approach must be adopted that incorporates technology, law, and user awareness.

Local governments and other public sector organisations in South Africa have inadequate cybersecurity budgets, lack of cybersecurity expertise, inadequate IT investments, and failure to apply the lessons learned from previous attacks Letseka (2022). In this regard, the South African local governments require multilayered cybersecurity strategies to combat these threats, including DDoS mitigation tools, traffic filtering and cleaning services, real-time monitoring and incident response protocols. One such strategy is a staff training and awareness campaigns of cybersecurity that will engage the staff members. In this regard, this dissertation present different strategies.

Local governments should use supplier verification systems and secure supplier databases, enforce multifactor authentication (MFA) for email accounts, establish multilevel approval procedures for financial transactions, implement email authentication protocols (SPF, DKIM, DMARC), train staff on awareness of BEC on a regular basis, and work with national security agencies like CSIRT and SABRIC to lower the risk of BEC.

3.3 Cybersecurity risks and vulnerabilities

3.3.1. Risks

Cyber risk encompasses a broad spectrum of threats associated with the use of information systems and digital technologies. Unauthorised access, data breaches, service interruptions, and cyber fraud are some of these risks, which can have serious negative effects on operations, finances, and reputation. The risk of cyberbullying is increasing in tandem with the growing reliance on digital platforms for data storage, trade, and communication. Cyber risk is defined by the National Institute of Standards Technology (NIST, 2011) as any possible negative impact that an information system failure could have on an organisation's operations, assets, or people.

Rapid service digitisation, widespread use of mobile devices, and cloud adoption in South Africa have increased the reach of attacks throughout the country. Because of this, the nation is now the target of sophisticated cyber-threats, necessitating a thorough understanding and management of cyber risks. Cyber risks are separated into several categories, each of which represents potential damage. Business process disruptions caused by system malfunctions or cyberattacks are called operational risks.

Reputational risk occurs when violations undermine stakeholder and public trust. Violating data protection laws and regulatory requirements, which can result in fines and sanctions, is part of the risk of legal and compliance issues. Intellectual property theft and spying frequently result in strategic risks that affect long-term objectives and competitive positioning. ISO / IEC 27005 provides a framework for recognising and categorising these risks as provided by ISO/IEC 27005 (ISO, 2018), allowing organisations to prioritise their mitigation efforts. Comprehending these categories is crucial to formulating focused cybersecurity strategies and efficiently allocating resources.

South Africa's distinct socio-economic and technological environment shapes the country's cybercrime risk landscape. Cybercrime, such as ransomware attacks, phishing campaigns, and business email compromise (BEC), has increased. South Africa is among the nations most affected by cyber risks (Interpol, 2021). The 2019 ransomware attack in Johannesburg is a notable example, as it revealed weaknesses in the public sector's IT infrastructure and interfered with municipal services. According to SABRIC (2024), losses from financial crimes in 2023 totalled R3.3 billion, and digital banking fraud increased by 45% annually. These incidents demonstrate the impact of cyber risks on public and private organisations and highlight the urgent need for strong cybersecurity measures.

South African regulatory bodies have strengthened cybersecurity governance through a number of actions in response to increased cyber risk. The Prudential Authority (PA) and the Financial Sector Regulatory Authority (FSCA) unveiled the 2024 Joint Standard 2, which requires financial institutions to implement risk-based cybersecurity procedures. The South African Reserve Bank (SARB) is working to improve the cybersecurity of payment systems. These guidelines support an organised approach to risk management and are in compliance with

international standards such as NIST and ISO/IEC 27005. Sharing of threat intelligence and coordinated incident response to incidents is made easier by institutional frameworks such as SABRIC and the Computer Security Incident Response Team (CSIRT). These initiatives are a major step toward ensuring cross-sector regulatory compliance and improving the resilience of national networks.

A multilayered approach that takes into account organisational, technical, and regulatory factors is necessary for strategic recommendations for risk reduction. To systematically identify, assess, and manage risks, organisations must implement risk management frameworks such as ISO/IEC 27005 and NIST SP 800-30. By continuously confirming user identities and access permissions, a zero-trust architecture can improve security. To close skill gaps, workforce development and cybersecurity education must be prioritised. To promote information exchange and collaborative defence projects, public-private partnerships must be reinforced. Furthermore, to maintain a proactive cybersecurity posture, regular security audits, penetration tests, and incident response planning are necessary (Microsoft, 2024; OWASP, 2023).

3.3.2. Vulnerabilities

According to NIST (2012), a vulnerability is defined as a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited. Understanding and addressing these vulnerabilities is essential to maintain the confidentiality, integrity, and availability of digital assets. These vulnerabilities can be caused by poor coding practices, incorrect configuration, outdated software, or lack of security controls. With the speed of digital transformation, cybersecurity vulnerabilities are exposed to increasing frequency, making them a major concern for both organisations and governments.

Understanding these vulnerabilities and addressing them is essential to maintaining the confidentiality, integrity, and availability of digital assets. Cybersecurity vulnerabilities can be classified into several categories based on their origin and impact. Common types include software vulnerabilities such as buffer overflows and injection errors, hardware vulnerabilities such as firmware bugs, configuration vulnerabilities, including default passwords and open ports, and human-related vulnerabilities such as social engineering and bad password practices.

The OWASP Top 10 (2023) provides a widely accepted classification of Web Application Vulnerabilities and highlights problems such as broken access control, cryptographic errors, and unsafe design. ISO/IEC 27005 (2018) emphasises the importance of identifying and classifying vulnerabilities to support effective risk management. The classification allows organisations to prioritise remediation efforts and allocate resources efficiently.

The consequences of cybersecurity vulnerabilities

- **Effect on the provision of Services:** Cybersecurity breaches can interrupt services, leading to significant downtime. For example, systems in charge of public safety, water supply and waste management can become paralysed by cyberattacks against local governments (Nhlapo, 2022). Long-term interruptions of service can cause public discontent and undermine trust.
- **Liability and monetary loss:** The financial implications of data breaches can be staggering. The Ponemon Institute estimates that an organisation's average cost for a data breach is around \$3.86 million (Ponemon Institute, 2021). Local governments are not immune from these costs; they face expenses related to recovery, remediation, and potential legal liabilities arising from breaches of citizen data.
- **Erosion of public trust:** Continuous cyberattacks can severely erode public trust in local governments. Citizens trust local authorities to protect their personal data. This trust is lost when strong cybersecurity is not maintained, which can result in PR disasters or public relations crisis and possibly affect future voter turnout and participation (Hussein & Ndlovu, 2021).

3.3.3. Recommendations

The human factor is often considered the most vulnerable aspect of cybersecurity. Social engineering attacks exploit this weakness by manipulating individuals to provide sensitive information. Training and awareness initiatives foster a culture of cybersecurity knowledge, which is crucial to mitigating social engineering risks. Ongoing training programmes must be established to inform employees about the prevalent tactics used by cybercriminals, including phishing, pretexting, and baiting. (Peltier, 2016). The latter could assist in dealing with vulnerabilities that could exist as it will increase resilience and inform employees to be more

aware and able to identify suspicious behaviours. In this regard, employees will respond effectively and are empowered to serve as the initial line of defence against possible threats.

3.4 Cybersecurity Theories, Models and Frameworks

The fundamental instruments for developing and implementing security strategies are cybersecurity models and frameworks. Models are theoretical frameworks that specify how security principles, such as availability, confidentiality, and integrity, should be applied to systems. Instead, frameworks are best-practices and structured guidelines that translate these ideas into procedures and actions. Frameworks are useful and operational, while models are conceptual and abstract (Sommestad, 2012; Conti et al., 2016;). Despite these differences, most cyber security professionals frequently use the terms interchangeably in policy and practice rather than making a clear distinction between them (Boyson, 2014).

3.5.1. Theories

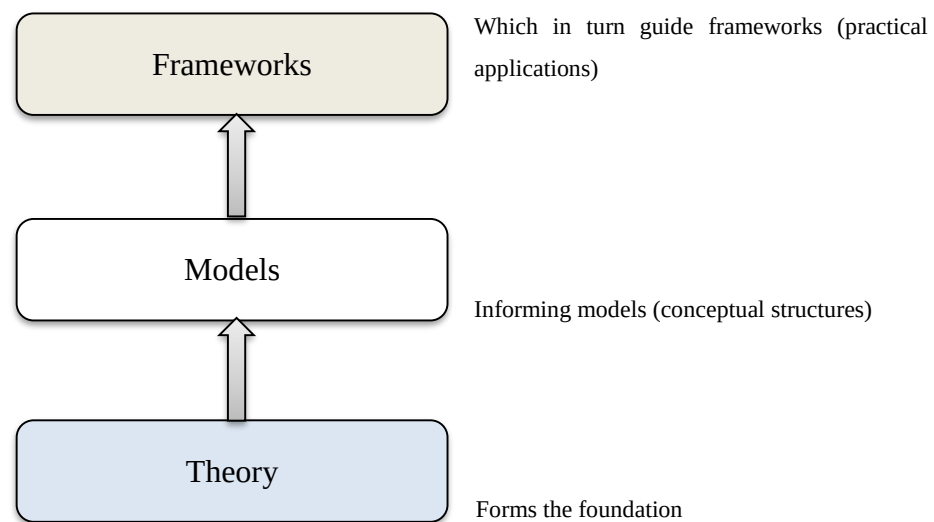


Figure 3-2: Relationship between Theory, Models, and Frameworks (Source: Author)

Figure 3-2 illustrates the hierarchical relationships in which cyber-security theory informs the development of models and enables the creation and implementation. The following theories are key in cybersecurity especially for local government context:

- **The Protection Motivation Theory (PMT)** – highlights how people react to perceived threats by appealing to their fear and resilience mechanisms (Rogers

1975). It is particularly helpful in understanding how users react to malicious software and phishing scams (Ifinedo, 2012). Its strength is the capacity to explain why people adopt protective behaviours when they perceive real threats and think that they work (Rogers, 1975). Unfortunately, PMT can oversimplify user behaviour and cause desensitisation and avoidance (Johnston & Warkentin, 2010).

- **The Theory of Planned Behaviour (TPB)** – focusses on behavioural intentions influenced by attitudes, subjective norms, and perceived control (Safa et al., 2016). It helps with forecasting the adherence to security policies. Its strength is on validating and demonstrating high degree of effectiveness in forecasting policy compliance (Safa et al., 2016). Unfortunately, TPB holds that high-stress or ambiguous cyber environments impair the ability to make logical decisions (Herath & Rao, 2009).
- **The Theory of Sociotechnical Systems (STS)** – takes a more comprehensive view by combining organisational, technical, and human elements to support a comprehensive security posture, the (Soomro et al., 2016). Its strength is show that technical fixes alone are insufficient without considering organisational and human dynamics (Soomro et al., 2016). Unfortunately, TSS are challenging to implement due to their complexity and the requirement for interdisciplinary collaboration (Soomro et al., 2016).
- **The Human-Climate Security Model (HCSM)** – emphasises empowerment and training, recasting users as active defenders as opposed to passive vulnerabilities (Pfleeger et al., 2014). Its strength is on the successful reduction of internal threats by encouraging a culture of accountability and awareness, the human-centric security model is especially (Pleeger et al., 2014). Unfortunately, HCSM requires substantial cultural shifts and ongoing training expenditures that could be costly (Pfleeger et al., 2014).
- **The Cybersecurity Maturity Model (C2M2)** – was created for organisational evaluation with an emphasis on the cybersecurity maturity of critical infrastructure (DOE, 2014). Its strength is to offer a well-organised framework to assess and improve cybersecurity readiness (DOE, 2014). Unfortunately, C2M2 is primarily

designed for large corporations and could not be easily scaled to SMEs or noncritical industries (DOE, 2014).

Moreover, since cyber risk is multifaceted, cybersecurity theories vary greatly in their areas of emphasis. Table 3-2 illustrates the comparative table is that indicate the strengths, weaknesses, and focus of each theory.

Table 3-2: Comparative Analysis of Cybersecurity Theories

Theory	Focus Area	Strengths	Limitations
PMT	Behavioural response to perceived threats	Explains motivation for protective actions; useful in phishing and malware contexts	May oversimplify behaviour; relies heavily on fear appeals
TPB	Behavioural intentions based on attitudes and norms	Predicts compliance with security policies; validated across contexts	Assumes rational decision-making; limited in high-stress scenarios
STS	Integration of human, organisational, and technical elements	Promotes a holistic security posture; considers organisational culture	Complex to implement; requires interdisciplinary collaboration
HCSM	Empowerment and training of users as security assets	Reduces insider threats; fosters responsibility and awareness	Resource-intensive; requires cultural change
C2M2	Evaluation of organisational cybersecurity maturity	Structured framework for readiness; applicable to critical infrastructure	Primarily suited for large organisations; limited scalability

The best option for improving the cybersecurity outcomes is to create a hybrid theory by integrating two or more theories. For example, by connecting emotions and cognitive factors, the combination of PMT and TPB can offer a more accurate understanding of users' motivation and intention (Ifinedo 2012; Safa et al., 2016). The systems that support resilient systems are both technically sound and easy to use, thanks to the application of TSS and HCSM (Pfleeger et al., 2014; Soomro et al., 2016;). Behavioural theories inform user engagement strategies, and C2M2 can be used as a foundation for organisational evaluation. In the end, using a multi-theoretical approach could enable local government to modify their cybersecurity plans in accordance with their particular risk profiles, technological settings, and human characteristics.

3.5.2. Models

Cybersecurity models provide an organised way to deal with digital risks, keep assets safe, and make sure that rules are followed and implement in best practices. They assist in finding weaknesses, and deal with threats. The models are based on confidentiality, integrity, and availability (CIA) well known as CIA triad, which are necessary for protecting both information and systems (Herrmann & Pridöhl, 2020). Table 3-3 explores key cybersecurity models, their applications, strengths, limitations, and relevance in today's threat landscape.

Table 3-3: Comparison of Cybersecurity Models

Model	Focus Area	Strengths	Limitations
NIST CSF	Risk Management	Flexible, widely adopted	No certification
ISO 27001	ISMS	International standard, certifiable	Resource-intensive
SOC2	Data Security	Trust-based, audit-driven	US-centric
FAIR	Risk Quantification	Financial impact analysis	Requires data modeling
MITRE ATT&CK	Threat Intelligence	Detailed tactics and techniques	Complex for beginners

Several organisations are using cybersecurity models because they want a more organised way to deal with digital threats. The NIST Cybersecurity Framework (CSF) and ISO/IEC 27001 are two examples of models that are widely used because they are flexible and recognised around the world. More than 85% of critical infrastructure organisations use the NIST CSF because it is flexible and fits risk management practices (NIST, 2024). ISO 27001 is preferred by larger organisations because its standards can be certified and are known throughout the world (ISO, 2022). These models help businesses establish security procedures that are always the same, respond better to incidents, and follow the rules.

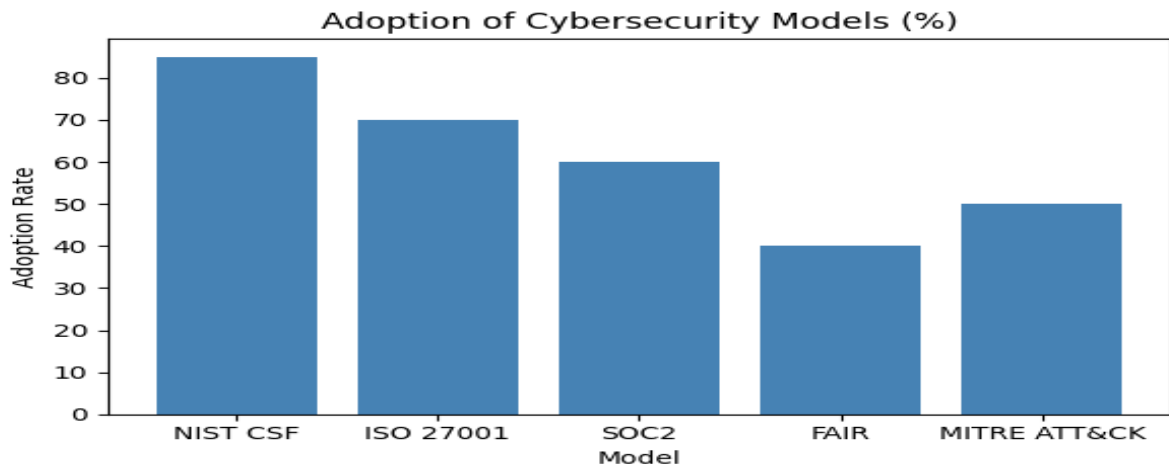


Figure 3-3: Adoption of cybersecurity models (Hasani et al., 2023)

Figure 3-3 illustrates the estimated adoption rate of major cybersecurity models. The adoption depends on the size, sector, and maturity of the organisation. ISO 27001 and SOC2 are examples of resource-intensive models that smaller organisations may have trouble with because of the costs of audits and paperwork. However, security teams that focus on measuring financial risk and gathering threat intelligence are increasingly using models like FAIR and MITRE ATT&CK (Jones & Ashenden, 2021; MITRE, 2023). Cybersecurity models have many benefits in the real world. They give a clear plan for implementing security controls, making risks more visible, and following the rules (NIST, 2024; ISO, 2022). Models such as NIST CSF and ISO 27001 allow organisations to establish security procedures that are the same across the board. This makes it easier to respond to incidents and stay safe.

Cybersecurity models can be difficult to put into practice, even though they have advantages. Many frameworks require a lot of resources, such as skilled workers, time, and money (ISO, 2022). ISO 27001 certification, for example, requires a lot of audits and paperwork, which can be difficult for small businesses to handle. SOC2 audits also require constant monitoring and reporting, which can put a strain on operational capacity (AICPA, 2023). Another concern is adaptability. Some models may not change sufficiently rapidly to deal with new threats, such as AI-driven attacks or weaknesses in the supply chain (MITRE, 2023). Models like FAIR can help you determine how much risk you have, but they need accurate data inputs and may not work for all businesses (Jones & Ashenden, 2021). In addition, static models may not work well in environments where threats change all the time, so they need additional tools and

methods. The concerns that are specific to an industry also affect how well a model works. For example, PCI DSS is made for payment card data, but it might not cover all your cybersecurity needs (PCI SSC, 2023). The FFIEC CAT is also made for banks and other financial institutions, so it may not work for schools or hospitals. To avoid misalignment and inefficiencies, organisations must carefully consider how relevant a model is to their operational context (FFIEC, 2024).

In summary, cybersecurity models are important to protect digital assets and making sure that organisations can recover from attacks. These models help businesses deal with complicated threat landscapes and keep their operations running by giving them structured ways to manage risk (NIST, 2024; ISO, 2022). Using models such as NIST CSF, ISO 27001 and SOC2 helps businesses follow the rules and makes stakeholders feel more confident. These frameworks set clear standards for security practices, which helps organisations show that they are responsible and in charge (AICPA, 2023; HITRUST, 2024). In cybersecurity, you have to keep changing things all the time. As threats change, models need to be updated often and given new tools and sources of information. Organisations can remain proactive and strong by using both dynamic frameworks like MITRE ATT&CK and quantitative models like FAIR (MITRE, 2023; Jones & Ashenden, 2021).

3.5.3. Cybersecurity frameworks

Cybersecurity frameworks (CSF) are organised rules that help organisations control online threats, safeguard data, and maintain operational stability. An effective CSF must include many essential components that ensure thorough participation and comprehension. For example:

- A good and effective framework should emanate from a risk assessment and analysis. The latter necessitates complete evaluations to identify organisation-specific threats and vulnerabilities. In this regard, facilitate the creation of customised awareness campaigns (NIST, 2020). This understanding of risks establishes the basis for specific learning objectives.
- The framework must explicitly define the intended behavioural results, emphasising the skills and knowledge necessary to counteract cyber risks (Anderson & Krathwohl, 2001).

- The framework content must align with the organisation's culture and employee experiences, incorporating applicable scenarios and terminology. This significance improves engagement and retention (Cone et al., 2007).
- The framework should be able to provide feedback obtained from allowing participants to gauge their understanding, while allowing administrators to track progress and effectiveness (Fernandez et al., 2019).
- The framework should use the game features such as points, levels, challenges, and prizes to convert conventional training into an engaging and motivating experience (Werbach & Hunter, 2012).

Cybersecurity frameworks provide businesses with a formal way to check their security processes, find any holes, put in place steps to stop them from happening, and ensure that they follow the rules. The following varieties of cybersecurity frameworks:

(i) The NIST Cybersecurity Framework (White & Sjelin, 2022).

It gives organisations in various industries a complete framework to deal with cybersecurity issues. Key components include the framework core that comprises five main functions:

- Identify – creates awareness of the environment of the organisation to control the risk of cybersecurity. The framework's identification function helps organisations find susceptible assets by promoting asset management.
- Protect – puts safety measures in place to ensure that important infrastructure services are always available. Every level of an organisation looks at and manages risks, which allows them to set priorities based on how much risk they can handle.
- Detect – creates the appropriate actions to determine whether a cybersecurity incident has occurred. The detection function places a lot of emphasis on threat intelligence and constant monitoring.
- Respond – addresses identified cybersecurity issues. It suggests making plans and being prepared to deal with and recover from attacks.
- Recover – makes preparation for how to bounce back and get back on track.

The framework implementation tiers range from Partial (Tier 1), Risk-Informed (Tier 2), Repeatable (Tier 3), and Adaptive (Tier 4). These tiers let the organisations see how well they can adapt, and profiles that help to customise alignments with organisational needs, risk tolerance, and resources. An example, of using the NIST framework as an evaluation tool in the local government was conducted in a study that aimed at assessing the cyber security posture of a local government organisation. The findings led to the organisation to strategically target areas related to their people, processes, and technologies, thus mitigating current and future threats. In this regard, NIST CSF is relevant in the local government setting.

(ii) ISO 27000 series framework (Meriah & Rabai, 2019).

Information Security Management System (ISMS) is highlighted as the foundation of the ISO 27000 series (ISO, 2021). It includes ISO 27001 (lists the steps needed to set up, maintain and improve an ISMS) and 27002 (provides advice and best practices for implementing security measures). The ISO 27000 series framework assists with regular risk assessments and the implementation of accepted controls to mitigate identified weaknesses. It keeps an eye on things so that an organisation can respond to new dangers as they arise. Furthermore, the controls in ISO 27002 help businesses protect themselves against data breaches. This standard uses a risk-based strategy to help businesses optimise their security procedures.

(iii) The Payment Card Industry Data Security Standard (PCI-DSS) (Yulianto, Lim & Soewito, 2016).

PCI-DSS gives important rules to businesses dealing with credit card information just like local municipality. The key components include twelve core requirements that cover methods for managing data security, such as setting up access controls and keeping an eye on things. In addressing vulnerabilities, threats, attacks, and risks PCI conducts vulnerability scans to find flaws in the systems that handle cardholder data. PCI-DSS deals with risks to payment processing by implementing strong compliance procedures in place. The framework lists ways to protect against data breaches and

regular checks to see if payment security standards are being met in light of new dangers.

(iv) Control Objectives for Information and Related Technologies (COBIT) (Wabiser & Singgalen, 2022).

COBIT is a set of rules for running business IT. Its important parts include management objectives that set governance, goals that ensure that IT and business goals are in line with each other and the framework components. COBIT addressing vulnerabilities by conducting risk management techniques that help companies find and fix weaknesses. COBIT's principles help people understand and deal with technological dangers and does this in systematic ways to control incidents. The framework employs a sensible risk management strategy that improves overall IT governance.

(v) HITRUST Common Security Framework ((Liñan-Acosta, Bazalar-Gonzales & Santisteban, 2025)).

The HITRUST CSF brings together a number of compliance criteria that are important for the healthcare industry (HITRUST Alliance, 2021). HITRUST key components include comprehensive compliance that consolidates several rules to facilitate the management of security obligations and a certification programme that ensures that everything is in order by going through a comprehensive evaluation procedure. HITRUST uses extensive risk assessment techniques that focus on keeping data safe. It encourages constant monitoring of risks within and outside the organisation. Best practices have been established to reduce the chance of attacks on sensitive data. It provides an organised way to deal with the risks that come with following the rules and keeping things safe.

(vi) The Cloud Controls Matrix (CCM) (Chandra, 2020).

The Cloud Security Alliance designed the Cloud Controls Matrix (CCM) to help with cloud computing settings (CSA, 2021). Its key components include control domains, which are groups of domains that provide security controls for cloud services, and mapping capabilities that make it easier to meet many different regulatory and compliance needs. Organisations using CCM CSF check cloud services against

established control standards and determine any risks that are unique to the cloud and provide advice on how to reduce the risks. It provides organisations with a way to create robust security procedures to protect their cloud infrastructure against attacks. However, cloud environments should have frequent risk assessments that are particular to them.

(vii) Essential 8 (Aman & Al Shukaili, 2021).

The Australian Cyber Security Centre came up with Essential 8, which lists ways to protect against cyberattacks (Australian Cyber Security Centre, 2021). The key components of this framework include eight strategies that focus on the basics, such as whitelisting applications, patching, and using multiple factors for authentication. It uses standard cybersecurity procedures to find and fix weaknesses. It helps businesses find and implement the measures they need to deal with risks.

(viii) Cyber Essentials (Calder, 2023).

The Cyber Essentials programme is a government-backed effort to make fundamental cybersecurity measures better for businesses (UK National Cyber Security Centre, 2021). The key components include five important controls, which are edge firewalls, secure configuration, user access control, and virus prevention. It encourages regular checks and updates for vulnerabilities to help organisations to learn about typical cyber dangers and how to protect themselves from them. It uses essential controls to protect organisations from attacks by focussing on practical solutions and encourages the inclusion of cybersecurity in larger risk management activities.

(ix) South Africa's cybersecurity framework (Gcaza & Von Solms, 2017).

The South African CSF was launched by the National Department of Communications and Digital Technologies in 2020. It aims to improve the country's overall cybersecurity posture by coordinating public and commercial sectors to cooperate together. It shows national assessments that identify problems in critical areas. It sets up early warning systems to deal with and reduce new threats. Its framework that work to ensure that all sectors use the same ways to respond to incidents and promote a complete national risk management framework to make the country more resilient.

(x) The Five-C Model (Mathew, 2023).

The Five-C CSF is a useful way to think about cybersecurity since it has five main parts: Change, Compliance, Cost, Continuity, and Coverage (ISO, 2021). Key parts include change that stresses that cybersecurity practices are always getting better whereas compliance stresses following rules and laws; on the other hand, cost look at how cybersecurity projects affect the budget, continuity place business continuity and catastrophe recovery strategies at the top of the list, and lastly, coverage ensure that security measures are in place in all parts of the organisation. Five C has to do with how to handle vulnerabilities so that they can adapt to changes. It uses regular evaluations to make people more aware of attacks that may be present in the environment. It helps to think about how to respond to attacks and to reduce any attack effects. It gives a complete picture of risk management by combining costs and compliance.

(xi) Service Organization Control (SOC) (Schoenfeld, 2024).

Service Organisation Control (SOC) reports look at how a service organisation's controls work with the internal controls of user entities over security and financial reporting (AICPA, 2020). It comprises Type I and Type II Reports. In Type I reports it show how the controls worked at a certain time, whereas in Type II reports it looks at how well the controls worked over a certain period of time. SOC reports assess the effectiveness of controls in addressing known vulnerabilities and conduct extensive reviews informing organisations about potential threats. It provides information on the security protocols and problems service providers are facing.

An overview of the cybersecurity frameworks examined is provided in Table 3-4 along with information on their key components and how they address risks, threats, vulnerabilities, and attacks.

Table 3-4: An overview of the cybersecurity frameworks

Framework	Key Components	Addressing Vulnerabilities	Addressing Threats	Addressing Attacks	Addressing Risks
NIST Cybersecurity Framework	Five core functions: Identify, Protect, Detect, Respond, Recover	Identified through risk assessments and asset inventories	Managed through proactive monitoring and threat intelligence	Emphasis on response and recovery processes	Organisations prioritise actions based on assessed risk
ISO 27001 and 27002	Establishes ISMS	Conduct regular risk assessments to identify vulnerabilities	Ongoing surveillance for emerging threats	Provides controls to protect against data breaches	Using a risk-based approach for security control
PCI-DSS	Twelve core requirements for handling card data	Regular vulnerability scans	Addresses threats related to payment processing	Outlines protective measures against data breaches	Regular compliance assessments for emerging risks
COBIT	Governance framework for enterprise IT	Identifies vulnerabilities through risk management processes	Promotes understanding of technological threats	Provides structures for incident control management	Practical risk management approach for enhanced governance
HITRUST CSF	Consolidates multiple compliance standards	Implements comprehensive risk assessment processes	Continuous surveillance of internal/external threats	Best practices to minimise risk of attacks	Structured approach to managing compliance-related risks
Cloud Controls Matrix (CCM)	Security controls specific to cloud computing	Assesses cloud services against control requirements	Focus on cloud-specific threats	Strong security practices for cloud infrastructure	Regular risk assessments tailored to cloud environments
CMMC 2.0	Maturity Levels for cybersecurity practices	Requires evaluation of vulnerabilities for certification	Best Practices Related to defence contracts	Emphasis on preparedness and response strategies	Continuous cybersecurity risk evaluations
Essential 8	Eight strategies for mitigating cyber threats	Directs implementation of basic cybersecurity practices	Identifies the necessary controls for threat management	Measures to Reduce Risks from common attack vectors	Supports the overall risk reduction strategy

Cyber Essentials	Five key controls	Promotes regular assessments for vulnerabilities	Awareness of common cyber threats	Measures to prevent attacks with practical solutions	Encourages integration of cybersecurity into risk management
South African Cybersecurity Framework	National coordination for cybersecurity	National vulnerabilities assessments of vulnerabilities	Early warning mechanisms for threats	Standardised incident response strategies	Comprehensive national risk management framework
Five C Model	Five key dimensions for cybersecurity management	Adapts to vulnerabilities through management	Regular assessments promote awareness of threats	Considers response strategies to minimise impact	Holistic view of risk management integrating costs/compliance
Centre for Internet Security Controls Framework	Top 20 cybersecurity best practices	Monitors and remediates vulnerabilities	Provides guidelines for threat hunting	Focusses on mitigating attacks with preventive controls	Integrates risk management with control implementations
Service Organization Control (SOC)	Type I and Type II Reports	Evaluate the effectiveness of controls against vulnerabilities	Provides information on potential threats	Transparency in Security Controls and incidents	Helps to understand the risks related to third-party providers

3.5.4. Recommendations

More organisations are adopting hybrid models that combine different models to meet their specific needs. This allows them to create cybersecurity strategies that are customised to their needs and that balance compliance, operational efficiency, and threat resilience. So, the recommendations say that choosing the right cybersecurity models is an important part of well-managed risk. Before choosing a model, businesses should think about their industry needs, legal requirements, and level of operational maturity. ISO 27001 is great for compliance across borders, while NIST CSF is better for risk management that can change between sectors (ISO, 2022; NIST, 2024).

Combining different frameworks can make cybersecurity more resilient. Organisations can better make decisions and use their resources by combining NIST CSF with FAIR. This is because it aligns qualitative controls with quantitative risk analysis (Jones & Ashenden, 2021). Combining MITRE ATT&CK with CIS Controls also makes it easier to find and deal with threats (MITRE, 2023; CIS, 2024). Training the workforce is very important for the model to work. To ensure that they follow the rules and are effective, employees need to know the principles and practices of the frameworks they choose. Regular training and awareness campaigns can reduce the number of mistakes people make and create a culture of security (AICPA, 2023; HITRUST, 2024). The cybersecurity strategy should include a plan for ongoing improvement. ISO 27001 and COBIT are two models that emphasise the need for regular assessments and updates to keep up with changing threats. To maintain strong security postures, organisations should conduct regular reviews, update controls, and compare their performance with others (ISACA, 2023; PCI SSC, 2023).

The future of cybersecurity is in hybrid models that use technical controls, behavioural analytics, and financial risk assessments together. Companies must put money into frameworks that can grow, work with other systems and support automation, real-time monitoring, and collaboration between sectors (ISACA, 2023; PCI SSC, 2023).

3.5 Cybersecurity best practices

Cybersecurity best practices are fundamental guidelines for protecting digital assets, ensuring data integrity, and encouraging an organisation-wide culture of cyber vigilance. Strong

cybersecurity measures are both strategically necessary and a governance imperative in the local government of South Africa.

Table 3-5: Summary of *cybersecurity* best practices

Cybersecurity Best Practice	Benefits	Challenges	Limitations
Strong Passwords & Multi-Factor Authentication (MFA).	Reduces the risk of unauthorised access.	Complexity for users to remember.	Protect against phishing or social engineering.
Regular Software Updates & Patching.	Fixes vulnerabilities.	Manage time and resources.	Updates have the potential to disrupt business operations.
Data Encryption.	Protect sensitive data.	This method may require a substantial amount of processing power.	It does not prevent data leaks if access controls are weak.
Regular Backups.	Disaster recovery if data are lost.	Time-consuming for large datasets	Backup data can also be compromised.
User Education & Training.	Reduce the risk of human error.	Time investment for training.	Users may not always retain or apply training.
Network Security Controls (Firewalls, IDS/IPS).	Monitors and controls incoming/outgoing network traffic.	Requires configuration and regular updates.	Not fool proof against sophisticated attacks.
Incident Response Planning.	Prepares the organisation for potential incidents.	It requires ongoing updates and training.	An effective response depends on prior preparation.
Access Control & Least Privilege.	Limits the potential damage of compromised accounts.	It can be complicated to implement.	Overly restrictive measures can hinder productivity.
Security Audits & Assessments.	Identifies vulnerabilities and compliance gaps.	Requires expert knowledge.	Resource-intensive and can be costly.

Tables 3-5 represent a high-level summary of common cybersecurity best practices, along with their advantages, challenges, and limitations. Each practice is crucial to building a robust cybersecurity posture tailored to the specific needs. there exist three main areas of cybersecurity best practices as briefly discussed below.

3.5.1. Technical safeguards

Technical safeguards encompass the tools and technologies used to protect networks, systems, and data from cyber threats. Effective technical measures are fundamental to establish a robust cybersecurity posture. For example:

- Firewalls act as barriers between trusted internal networks and untrusted external networks, filtering incoming and outgoing traffic based on predetermined security rules (Scarfone & Mell, 2007).
- Intrusion detection systems (IDS) complement firewalls by monitoring network activity to identify possible unauthorised access or anomalies (Tan et al., 2019). Research indicates that organisations employing a combination of firewalls and IDS witness improved network security outcomes (Reddy et al., 2020). However, maintaining these systems requires ongoing management and updates to adapt to emerging threats (Mavroeidis et al., 2021).
- Encryption is a critical best practice to protect sensitive data in transit and at rest. Data encryption ensures that even if a cybercriminal gains access to sensitive information, it remains unreadable without the correct decryption keys (Khan et al., 2021). Studies show that organisations that implement encryption see a significant decrease in data breaches and compliance-related issues (Almashaqbeh & Alzahrani, 2020). However, secure management of encryption keys presents a challenge, as mishandling can negate the benefits of encryption (Chow et al., 2018).
- A regular software and system update is vital to mitigate vulnerabilities. Security patches often address known vulnerabilities and protect against exploitation (Mouton et al., 2018). Research emphasises the importance of an effective patch management policy, noting that organisations with consistent update practices experience fewer security incidents (Tao et al., 2021). Challenges arise from ensuring that all systems are updated promptly, particularly in organisations with extensive legacy systems (Kaastra et al., 2021).

3.5.2. Administrative measures

Administrative measures refer to local government policies and processes that define how cybersecurity practices are implemented and managed. To be effective these policies should be enforced through:

- Conducting regular risk assessments enables organisations to identify vulnerabilities and prioritise resources effectively (ISO, 2018). A systematic risk

management approach helps organisations allocate resources efficiently and mitigate potential impacts (Doherty & Fulford, 2017). However, many organisations struggle with continuous risk assessments, often due to resource constraints or a lack of expertise (Purdy, 2010).

- Implementing robust access control measures minimises the risk of unauthorised access to sensitive information. Role-based access control (RBAC) allows organisations to grant access permissions based on user roles within the organisation (Sandhu et al., 2018). Research highlights that organisations that enforce strict access controls significantly reduce the risk of insider threats (Hahn et al., 2021). However, balancing security needs with user productivity remains a challenge (Wang et al., 2020).

3.5.3. User awareness initiatives

User awareness initiatives focus on educating employees about cybersecurity threats and best practices and fostering a security-centric culture within the organisation. Security awareness training is a vital component in reducing human error, which is often a significant factor in successful cyberattacks (Hadnagy, 2018). Training programmes can include workshops, online modules, and simulations to engage employees and reinforce best practices (Furnell, 2020). Studies indicate that regular training significantly improves the ability to recognise phishing attempts and other cyber threats (Braun et al., 2019). However, ensuring ongoing engagement and retention of knowledge is a common challenge (Rogers & Wainwright, 2021).

Phishing attacks remain one of the most prevalent threats to organisations and phishing awareness campaigns are conducted to deal with them. Campaigns aimed at increasing awareness of phishing tactics can empower employees to identify and report suspicious communications (Sätra et al., 2020). Research suggests that organisations that use simulation exercises and real-life examples used in campaigns have been shown to significantly reduce successful phishing attempts (Turgut & Yalçın, 2021). However, employees may become desensitised to frequent meetings. Training efforts require more innovative approaches to maintain their effectiveness (Jenkins et al., 2020).

Organisations face numerous challenges when implementing best-practices in cybersecurity. Common barriers include resource limitations, lack of executive support, and complexity of cybersecurity landscapes (Hadnagy, 2018). Furthermore, cultivating a culture of security awareness can be hampered by employee resistance, a lack of understanding, and inadequate engagement from the organisation's leadership (Levine & Reddick, 2019).

A comprehensive cybersecurity awareness strategy has many essential components that together create a unified educational programme (ISO/IEC 27001, 2013). These characteristics are essential to determine the effectiveness of gamification in educational initiatives.

- **Education and training:** The foundation of every cybersecurity awareness initiative is education and training. Employee training must encompass fundamental cybersecurity principles, prevalent risks, and optimal procedures for data protection (Hadnagy, 2018). Consistent training sessions can improve awareness of emerging problems and strengthen their ability to identify possible risks.
- **Communication:** Effective communication is crucial to improving employee awareness. Organisations must communicate policies, processes, and the importance of cybersecurity in both formal and informal settings (NIST, 2018). Concise communication reinforces the importance of cybersecurity measures and ensures that staff understand their responsibilities in protecting sensitive data.
- **Evaluation and feedback:** To ensure the effectiveness of a cybersecurity awareness campaign, continuous assessment and feedback methods must be established. Assessing the effectiveness of training through evaluations, surveys, and performance indicators facilitates the identification of improvement areas and subsequent improvements to the programme (O'Connor, 2019). Feedback loops are essential for the continuous improvement of training methods and materials.
- **Involvement:** Engagement is crucial in an effective awareness approach. Gamification strategies, such as quizzes, incentives, and leaderboards, can encourage employees to actively participate in training sessions. Involving workers in interactive experiences improves retention and cultivates a culture of cybersecurity knowledge (Deterding et al., 2011).

- Design considerations for gamification in cybersecurity awareness: organisations should examine many critical elements that affect the overall efficacy of organisation security awareness programmes (Kapp, 2012).
- Understanding the audience: Before implementing the gamification components, it is crucial to understand the target audience. Diverse personnel may possess various degrees of technological expertise and may react differently to gamification strategies. Customising information and challenges to align with the audience's abilities and preferences will improve engagement (Landers et al., 2017).
- Setting explicit objectives: Setting explicit objectives for the gamified experience is essential. The objectives must correspond to the general objectives of the cybersecurity awareness programme and delineate the anticipated learning outcomes or achievements of the participants (Sailer et al., 2017). Explicit objectives facilitate the evaluation of the effectiveness of the gamification initiative.
- Level of challenge: The challenge level in gamified activities must achieve equilibrium to maintain motivation without causing overload. An ideal challenge motivates participants to extend their limits while maintaining a sense of achievable success, fostering a constructive gaming atmosphere (Gee, 2008).
- Integration with existing training: Gamification needs to improve current training programmes rather than replace them. Organisations want to incorporate gamified components into their existing training framework, facilitating a synthesis of conventional techniques and interactive encounters (Muntean, 2011). Integration guarantees continuity and improves educational experience.
- Continuous updates: Cybersecurity threats are always developing; therefore, gamified information must be regularly updated to align with the latest trends and challenges related to cyber threats (Choo, 2016). Continuous updates ensure that employees are knowledgeable and equipped to address emerging risks.

3.6 Recommendation

Cybersecurity risks in local government institutions include a wide range of technical, behavioural, and organisational factors. These organisations often demonstrate an elevated risk profile attributable to factors such as human error, inadequate training, and a deficient security culture (Kshetri, 2019). So, any good cybersecurity plan needs to include both technological protections and actions that focus on people to fully address these weaknesses.

The Protection Motivation Theory (PMT) and the Theory of Planned Behaviour (TPB) are some of the theoretical frameworks that help us understand how people think about cybersecurity threats and what they do to protect themselves. For example, PMT talks about how threat appraisal and coping strategies affect people's motivation to adopt security behaviours (Rogers, 1983), while TPB talks about how attitudes, subjective norms, and perceived behavioural control shape people's intentions (Ajzen, 1991). These theories emphasise the need to design awareness campaigns that not only convey information but also facilitate significant behavioural transformation. In addition to these behavioural perspectives, Sociotechnical Systems Theory supports integrated strategies that take into account how people, technology, and organisational structures interact with each other in real time (Bostrom & Heinen, 1977). This method is especially useful in local government, where cybersecurity problems often come from technical systems that do not work well with human processes.

The Bell-LaPadula, Biba and Clark-Wilson models are the most important formal security models for information systems because they help keep data private, safe, and only accessible to the right people (Sandhu & Samarati, 1994). These models are theoretically sound, but when used in local government settings, they need to be simplified and adapted to meet the needs of the situation due to limited resources and different levels of technical skill.

The NIST Cybersecurity Framework (CSF), ISO/IEC 27001, and the CIS Controls are examples of internationally recognised frameworks that provide structured ways to deal with cybersecurity risks. These frameworks give you clear steps to take to find, protect, detect, respond to, and recover from cyber incidents. But its use in South African cities is still limited due to money problems and a lack of trained staff (Von Solms & Van Niekerk, 2013).

The idea of using gamification as a strategic tool to raise awareness of cybersecurity is being recommended. Gamification uses things such as rewards, competition, and feedback to get people involved and help them learn (Hamari, Koivisto & Sarsa, 2014). When combined with behavioural theories such as PMT and TPB, gamified interventions can foster a proactive security culture and mitigate risky behaviours among municipal employees.

The literature confirms that cybersecurity issues in the local government cannot be resolved solely by technological solutions. A comprehensive approach that integrates behavioural theory, organised frameworks, and engaging awareness methods, such as gamification, can allow municipalities to create robust cyber environments. The following chapters will turn these ideas into useful advice for creating and running gamified cybersecurity awareness programmes that are tailored to the specific needs of the local government of South Africa.

3.7 Cybersecurity strategies

Different cybersecurity strategies exist. Table 3-6 provide the summary of the cybersecurity strategies, along with their benefits, challenges, and limitations. To explore these strategies various training formats have been explored, including online modules, in-person workshops, and simulation exercises. Online training modules are among the most widely adopted methods for providing cybersecurity awareness training. They offer flexibility and scalability, allowing organisations to reach a broad audience (Sasse, 2020). Research by Wognum et al. (2021) highlights that interactive modules are particularly effective in engaging employees and improving retention of cybersecurity concepts. However, the effectiveness of online training often varies according to employee self-motivation and prior knowledge of cybersecurity (Granger et al., 2018). Through an in-person training programme, workshops provide an opportunity for interactive learning and immediate feedback.

Table 3-6: Summary of cybersecurity strategies

Cybersecurity Strategy	Benefits	Challenges	Limitations	References
Employee Training and Awareness	Enhances overall security posture, reduces human error, and promotes a security culture.	May require ongoing resources and time; varying effectiveness depending on engagement.	Cannot fully eliminate risks; relies on all employees participating.	Mitnick & Simon (2002); Hadnagy (2010)
Multi-Factor Authentication (MFA)	Provides an additional layer of security; reduces risk of unauthorised access.	Usability can be an issue; potential for user dislike.	Not fool proof; sophisticated attacks can bypass MFA.	Roopesh (2024)
Regular Software Updates	Mitigate vulnerabilities; ensures use of the latest features and security patches.	Requires ongoing attention and resources; complex for large systems.	Potential downtime during updates; risks from untested updates.	IJCRT (2023)
Network Security Solutions (Firewalls, IDS/IPS)	Monitors and protects network traffic; prevents unauthorised access.	It can be complex to configure and maintain; false positives can hinder operations.	Requires constant updates; can be bypassed by advanced attacks.	Roopesh (2024)
Incident Response Plans	Incident response plans offer a systematic method to reduce impact and speed up the recovery process after incidents.	Development and implementation can be resource-intensive; must be regularly tested.	Limited effectiveness if not followed properly; relies on timely activation.	Shostack (2014)
Data Encryption	Protect sensitive data in transit and at rest; builds trust with clients	Can slow down system performance; requires proper key management.	Complexity in management does not protect against endpoint vulnerabilities.	Roopesh (2024)
Regular Security Audits and Assessments	Identifies vulnerabilities, ensures compliance, and creates awareness of the security posture.	The process can be time-consuming and costly, depending on the expertise of the assessors.	The scope of the audit may limit its ability to capture emerging threats.	IJCRT (2023)
Cyber Threat Intelligence Sharing	Improves understanding of the threat landscape; improves proactive defences.	Sensitive data can be mishandled; requires trust and collaboration among entities.	It can be ineffective if organisations do not act on shared intelligence.	Shostack (2014)
Access Controls	Limits exposure to sensitive information; reduces insider threats.	Complexity in implementing granular access controls.	Difficult to enforce across diverse platforms; can impede productivity.	Kennedy et al. (2011)

According to D'Arcy et al. (2021), these workshops enable the incorporation of real-world scenarios, making the training more relatable and effective. Although in-person training can be resource intensive, it often results in higher levels of engagement compared to online programmes (Bleam et al., 2020). However, simulation exercises, including phishing simulations and incident response exercises, have become effective tools to raise awareness and assess employee behaviour in controlled environments (Chatchalermpon & Daengsi, 2021). Studies have shown that these exercises can greatly improve readiness to face real cyber threats (Rogers & Wainwright, 2019). However, careful planning is necessary to avoid psychological stress among participants (Davis, 2018).

Effective communication strategies are crucial to reinforce awareness of cybersecurity within organisations. These strategies include regular updates and newsletters that guide frequent communication about cybersecurity policies, updates, and emerging threats while keeping employees informed and vigilant (Notar & Padgett, 2019). A study by Albrechtslund et al. (2021) found that organisations that use regular newsletters see an improvement in employee awareness and compliance with cybersecurity measures. Lastly, awareness campaigns, such as security awareness month or themed campaigns surrounding specific threats, can engage employees and create a culture of security (El-Qassas et al., 2020). These campaigns often use posters, emails, and workshops to spread the word. However, organisations often face challenges in measuring the impact of such campaigns on behavioural change (Gupta et al., 2018).

Additionally, integrating cybersecurity awareness into the culture of local governments is essential to sustain long-term awareness efforts. A strong security culture encourages all employees to prioritise cybersecurity in their daily activities and will require leadership support, as leadership plays an important role in the promotion of a culture (Peters & Bansen, 2020). When local government leaders actively support and participate in cybersecurity initiatives, employees are more likely to participate in training and adhere to security policies (Renaud et al., 2021), and lastly, encouraging employee participation in cybersecurity initiatives can significantly improve awareness. Initiatives such as gamification and security champions programmes have been shown to increase engagement levels (Harris et al., 2021).

However, maintaining ongoing engagement can be challenging and requires continuous effort and innovation (Albu & Rizzo, 2020).

Despite the best efforts to implement these strategies, several challenges remain. Employee resistance to change, lack of time, and inadequate resources often hinder effective training and awareness initiatives (Ferrante et al., 2018). In this regard, measuring the success of cybersecurity awareness campaigns remains a complex task (Whitman & Mattord, 2020). Figure 3.4 illustrates essential components of cybersecurity awareness strategies which could easily be measured.



Figure 3-4: Components of the cybersecurity awareness strategy (Source: Author).

The protection of sensitive data, preserving digital infrastructure, and guaranteeing the continuation of public services. These components (as discussed below) allow the good cybersecurity measures to assist in proving a strong strategy.

- **Audience assessment:** Understanding the target audience is essential to the effectiveness of any awareness campaign. This analysis entails analysing the demographics, jobs, and current knowledge levels of workers. Customising content and delivery techniques to address the different needs of different groups, such as

IT personnel, management, and general employees, can noticeably improve training effectiveness (Bada et al., 2019).

- **Explicit objectives:** Establishing explicit and quantifiable objectives for the awareness strategy is crucial to guide the implementation process. The objectives should focus on the behaviours that the training intends to modify, such as identifying phishing attempts or implementing password management procedures (Tsohou et al., 2019). Establishing defined goals improves the evaluation and refinement of the plan.
- **Compelling content:** Engagement is a fundamental component of any awareness approach. The use of interactive information, including videos, infographics, and quizzes, can improve employee engagement and motivation (Hollis et al., 2018). Gamification advances this notion by using game-like features to enhance engagement and information retention.
- **Ongoing education:** Cybersecurity is a dynamic discipline that requires ongoing education. Strategies must include continuous training and refresher courses to keep staff informed about current risks, vulnerabilities, and best practices (Fischer, 2020). Using gamification can make ongoing learning more captivating and less tedious.

On-going education provides a clear delivery strategy for achieving a competent strategy. However, if the content is not compelling participant might neglect the education and training. The compelling content is provided through different strategies as discussed above. In this study a cybersecurity awareness compelling content was identified to be a gamified awareness training section. In this regard, designing considerations for gamified cybersecurity awareness strategies should be priority for developing and providing a compelling strategy. When designing gamified cybersecurity awareness tactics, several critical factors must be considered to improve effectiveness and participation:

- **Gameplay mechanics:** Integrating game components, such as points, badges, and leaderboards, can improve motivation for engagement and competitiveness among employees. Point systems enable employees to monitor their progress, while badges

offer visible acknowledgement of achievements. Leaderboards promote constructive competition and cultivate a sense of community among players (Deterding et al., 2011).

- **Narrative construction:** Narrative elements can substantially enhance engagement by immersing users in a story relevant to the material. Employing a narrative that mirrors typical workplace situations could offer a relevant framework for employees, improving the importance of the learning experience (Whitton, 2014).
- **Engaging challenges:** Gamification techniques must integrate interactive challenges that replicate authentic cybersecurity events, such as recognising phishing emails or responding to data breaches. This experiential method consolidates knowledge and allows participants to hone their abilities in a secure setting (Gee, 2003).
- **Feedback mechanisms:** Timely feedback is crucial for learning and improvement. Integrating tools for fast feedback, such as quizzes with instant scoring or comments, allows users to pinpoint areas for improvement and solidify their understanding of the information (Kang et al., 2020).
- **Accessibility and inclusion:** It is essential to ensure that gamified training programmes are accessible and inclusive to all employees. This process involves evaluating several learning modalities and providing material in numerous formats. Furthermore, we must tailor training to address diverse backgrounds and experiences in cybersecurity awareness (Sullivan et al., 2019).

Validation procedures are essential to confirm that the tactics carried out get the intended results. Validation techniques for gamified cybersecurity awareness strategies can use variety of methodologies to assess user engagement and information retention, namely:

- **Pre-and post-training evaluations:** Employing pre- and post-training evaluations helps measure employee knowledge before and after participation in gamified training. Evaluating results enables businesses to assess the efficacy of training material (Wang et al., 2016).

- **User feedback surveys:** Gathering user input via surveys and interviews is crucial to comprehending participants' experiences. Feedback offers insight into the strengths and flaws of gamification elements, facilitating ongoing improvement (Davis & Tullis, 2010).
- **Behavioural observations:** Monitoring employee behaviour at work before and after training can provide significant information on the practical effects of the gamified approach. For example, examining the frequency of reported phishing attempts or compliance with password regulations could determine the impact of training on behaviour (Bhana et al., 2022).
- **Longitudinal research:** Longitudinal studies can elucidate the lasting effects of gamified training on employee awareness and conduct. Organisations can determine the effectiveness of training by evaluating knowledge retention and behavioural modifications over time, thus identifying the need for refresher courses (Whitney, 2019).

3.8 Recommendation

Table 3-7: Comparison of Cybersecurity Models and Frameworks

Aspect	Model	Framework
Purpose	Conceptual understanding	Practical implementation
Focus	Security principles	Processes and controls
Examples	Bell-LaPadula, Biba, Clark-Wilson	NIST CSF, ISO/IEC 27001, CIS Controls

Cybersecurity theories support models and frameworks by providing conceptual explanations of threats, vulnerabilities, and controls (see Table 3-7). For instance, the Bell-LaPadula model, which uses the "no read, no write" rule to prevent access to unauthorised data, is informed by the secret theory (Bell & LaPadula, 1973). In a similar vein, integrity theory supports the Biba model, which uses the "no writing, no reading" principle to prevent data modification (Biba, 1977). These models serve as the foundation for systems like NIST's Cybersecurity Framework, which applies risk management theory to the protection of critical infrastructure, and ISO/IEC

27001, which integrates these principles into information security management systems (ISMSs) (NIST, 2018).

The National Cyber Security Policy Framework (NCPF) in South Africa serves as an example of how cybersecurity frameworks are used in public administration. The National Security Agency created the NCPF as a strategic objective, which includes fostering a culture of cyber security, coordinating the emergency response, and protecting vital information infrastructure (National Security Agency 2015). Through national cybersecurity surveys that evaluate organisational readiness and compliance with international standards such as NIST and ISO, the Scientific and Industrial Research Council (CSIR) highlighted the significance of the framework (CSIR, 2024). These initiatives demonstrate the incorporation of theoretical models into real-world governance structures. To create a robust cybersecurity system, theory, models, and frameworks must be integrated. The theory guarantees logical coherence and adaptability, models offer conceptual frameworks, and frameworks offer implementation pathways.

3.9 Conclusion

Cybersecurity is now a core requirement to protect sensitive information, securing digital systems, and ensure that essential services run without interruption. This study shows that effective cybersecurity strategies need to combine strong technical measures—such as multifactor authentication and data encryption—with approaches that focus on people, like employee training and awareness (Roopesh, 2024; Mitnick & Simon, 2002). Technology provides the backbone of security, but its success depends on how well employees understand and follow best practices, making an integrated approach essential.

Training and awareness programmes are key to reducing human error and building a culture of security. Different formats, online modules, workshops, and simulation exercises, offer unique benefits. Online modules are flexible and scalable (Sasse, 2020), while workshops and simulations provide hands-on learning and real-world scenarios (D’Arcy et al., 2021; Rogers & Wainwright, 2019). Gamification has become an innovative way to make training more engaging by using points, badges, and storytelling (Deterding et al., 2011; Whitton, 2014). However, these methods need careful design to ensure that they are inclusive and meaningful. Measuring the impact of these initiatives through assessments, feedback, and behavioural

observations is just as important as implementing them, as it helps organisations confirm that training leads to real improvements (Wang et al., 2016; Bhana et al., 2022).

Finally, building a strong cybersecurity posture requires more than tools and training; it needs a solid foundation of theory, models, and frameworks. Models like Bell-LaPadula and Biba set out principles of confidentiality and integrity (Bell & LaPadula, 1973; Biba, 1977), while frameworks such as NIST CSF and ISO/IEC 27001 turn those principles into practical steps (NIST, 2018). In South Africa, the National Cyber Security Policy Framework shows how global standards can be adapted to local needs (National Security Agency, 2015; CSIR, 2024). Combining technical controls, behavioural strategies, and continuous validation creates a resilient system that can keep up with evolving cyber threats.

CHAPTER 4

FINDINGS: SYSTEMATIC LITERATURE REVIEW

4.1 Introduction

The aim of this Chapter is to present the work conducted to achieve TO1b and TO2:

TO1b: *“To explore the literature on design considerations, and validation methods for the development of cybersecurity awareness strategies using gamification.”*

TO2: *“To explore the literature on the gamification tools and techniques that can be used to increase awareness of cybersecurity. Then identify and select cybersecurity games that are suitable for the specific context of the cybersecurity awareness context.”*

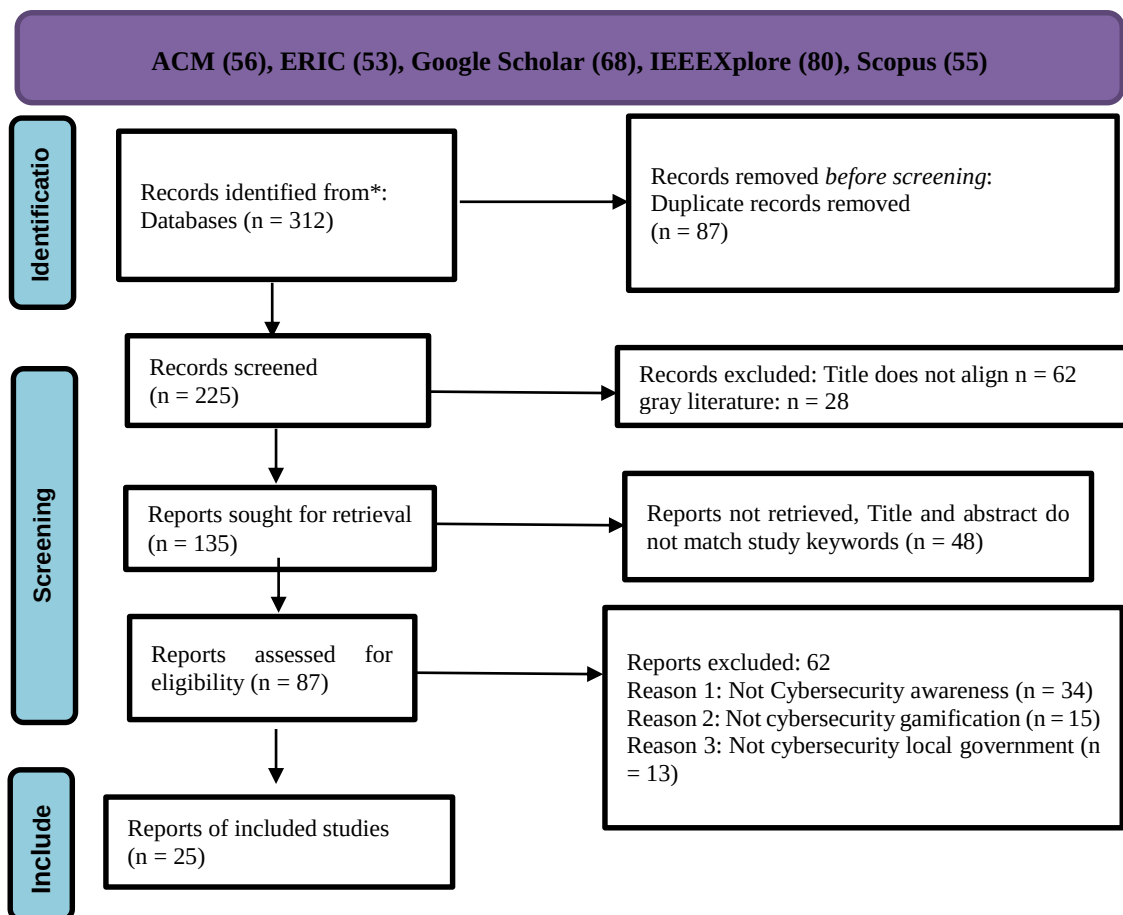


Figure 4-1: Components of the cybersecurity awareness strategy (Source: Chapter 2).

In Chapter 3, a scoping literature review was conducted to achieve first section of the first theoretical objective (TO1a) and to identify and select a cybersecurity game that is suitable for the specific context of cybersecurity awareness in this case local government (TO2b). Furthermore, in this Chapter, a systematic literature review (SLR) was used to achieve TO1b and TO2a. In this regard, in Chapter 2 a PRISMA framework for conducting SLR was introduced and is highlighted in Figure 4-1. Furthermore, this Chapter synthesis reports of 25 studies to determine the design considerations, and validation methods for the development of cybersecurity awareness strategies using gamification.

4.2 Identify and select cybersecurity games that are suitable for the specific context of the cybersecurity awareness context

The use of game design elements outside of games has become a powerful way to increase motivation, participation, and learning in many areas, such as cybersecurity training and games. In South Africa, where people know less about cybersecurity, gamification could bring fun and interactive way to train individuals than using traditional training methods.

Gamification is the process of adding gaming elements in a non-game environment to make users more interested and motivated. Deterding et al. (2011) assert that gaming leverages intrinsic motivations to foster engaging experiences through elements such as scorecards, leaderboards, and challenges. When used to raise awareness of cybersecurity, games help people learn about security protocols and change their behaviour to be more protective. In their study, Deterding et al. (2011) found that people were more likely to remember information when it was presented in a game-like way. This method is especially useful for local government workers who may have different levels of knowledge, education attainment, especially cybersecurity knowledge. In this regard, the principles of effective gamification are grounded in psychological theories of learning and motivation.

Gamification provides several advantageous effects to improve cybersecurity efforts within local governments, including the following.

- **Enhanced Engagement:** Gamified training programmes attract employees' attention and promote active participation, leading to elevated completion rates and efficacy (Hamari et al., 2014).
- **Enhanced retention:** Research indicates that recognition improves information retention by making learning more participatory and memorable (Wang et al., 2016).
- **Real-time feedback:** Gamification provides immediate feedback on performance through tests and challenges, helping people recognise areas for improvement (Kapp, 2012).
- **Cultural transformation:** Integrating gamified components into cybersecurity training helps cultivate a security-conscious culture within local government agencies by making security practices more accessible and relevant (Rogers et al., 2020).
- **Cost-effectiveness:** The use of digital gamified training platforms may be more economical than conventional training techniques, particularly in resource-constrained areas (Glover, 2013).

Integration of gamification in cybersecurity awareness training has emerged as an effective method to improve user engagement and cultivate a proactive culture of security awareness among individuals and organisations (Deterding et al., 2011). By using gamified components, such as prizes, challenges, and interactive simulations in cybersecurity training and awareness initiatives, organisations can convert typically monotonous and daunting material into captivating experiences that encourage employees to learn and embrace secure practices (Shead et al., 2020). This innovative method takes advantage of intrinsic motivations and cultivates a more engaging learning environment, allowing participants to grasp complex cybersecurity topics and identify possible risks proficiently (Bălăceanu & Iliescu, 2018). As cyber risks increase, gamification becomes an essential tool to allow employees to actively defend sensitive information and systems, thus improving the overall cybersecurity posture of enterprises. Gamification employs game features in nongaming environments to enhance engagement, motivation, and learning. In cybersecurity awareness, gamification can

effectively convert standard training sessions into captivating and participatory experiences (Deterding et al., 2011).

The effective execution of cybersecurity gamification in the local government is based on many essential strategies.

- **Evaluating learning objectives:** Local governments must define certain cybersecurity skills and knowledge that they want to improve through gamified training (Wang et al., 2016).
- **The content and mechanics development:** Producing captivating and pertinent information is essential. Customising the game mechanics to align with the intended learning objectives and the specific audience is crucial (Deterding et al., 2011).
- **Pilot evaluation:** Preliminary pilot initiatives can assess staff participation and efficacy prior to larger deployment. Participant feedback can guide enhancements and scalability.
- **Ongoing assessment:** Local governments must implement systems for continuous evaluation of the effectiveness of gamified training, adapting the programme in response to employee input, and developing cybersecurity risks (Rogers et al., 2020).

The integration of games into cybersecurity training revitalises what was once a dry, compliance-orientated exercise into a learning-centric experience. Using point systems, leaderboards, badges, and interactive simulations, organisations use both internal and external motivations to drive higher participation rates and deeper security best practices. Effective gamification combines lightweight mechanics such as micro-challenges and quick-win rewards with more immersive serious game experiences that simulate real-world threats. This mixed approach not only supports long-term commitment but also ensures that employees develop critical thinking and decision-making skills needed to identify and respond to evolving cyber threats.

In addition, Hamari et al. (2014) state that for gamification to work, it needs to make people feel like they have accomplished something, encourage teamwork, and spark competition. Local governments can use these ideas in cybersecurity training by using simulations that mimic real-world cyber threats. This will give employees hands-on experience in detecting and dealing with these kinds of problem. Employees not only learn about cybersecurity best practices through role-playing or interactive quizzes, but also use what they learn, which strengthens their knowledge and makes them more aware of their surroundings. Furthermore, the fact that gamification is a group activity encourages employees to work together and talk to each other, both of which are important for improving the overall cybersecurity posture.

A review of national and international studies that have looked at gamified cybersecurity tactics opens the discussion, highlighting areas that lack empirical support. After that, it focusses only on South Africa and finds shortcomings in the wider public sector's use, development, and assessment of gamification tools. Implementing gamified awareness programmes is hampered in local government institutions by issues such as digital literacy, fragmented policies, and lack of funding. These gaps highlight the need for context-sensitive research and customised solutions that consider the realities of local governments in South African local governments.

Similar studies and identified gaps in cybersecurity gamification within the current research landscape. Table 4.1 provides a summary of similar studies and identifies gaps in cybersecurity gamification within the current research landscape.

Table 4-1: A summary of similar studies and identifies gaps

Aspect	Similar studies	Identified gaps
Foundational Understanding of Gamification	Deterding et al., 2011: Described the concept and potential of gamification in various domains, emphasising its role in education and user engagement.	Specific exploration of gamification in cybersecurity, especially in local governments in South African local governments, is limited.
User Engagement and Motivation	Hamari et al., 2014: Analysed the impact on motivation and engagement in various sectors, confirming general effectiveness.	Research lacks a focus on long-term sustainability and effectiveness in cybersecurity-specific training contexts.
Cybersecurity Context in South Africa	Van Niekerk & Von Solms, 2015: Investigated cybersecurity awareness efforts in South Africa, noting challenges in engaging local sectors.	Absence of gamification strategies tailored to South Africa's local government-specific cybersecurity needs.
Adoption in Local Government	Studies highlight the general advantages of gamification in government settings (Monyamane & Mphahlele, 2020).	Empirical evaluations are needed to grasp the applicability and scalability in local governments.
Evaluation and Sustainability Frameworks	Existing frameworks internationally assess gamification strategies (Deterding et al., 2011).	Need for models that incorporate regional-specific cybersecurity challenges and resource constraints.

4.3 Design considerations and validation methods for the development and usage of cybersecurity awareness strategies using gamification

Gamification tools to improve cybersecurity awareness are essential for protecting organisations against a constantly changing threat environment. Although technical solutions are crucial, cultivating a culture of awareness and vigilance among employees is equally vital. Conventional training approaches frequently fail to appeal to employees, resulting in difficulties in information retention and compliance (Baker et al., 2020). As a result, gamification has become a useful way to increase interest, motivation, and learning outcomes in cybersecurity training.

Gamification tools generally integrate diverse design components, namely, points, badges, and leaderboards (PBL). These reward mechanisms offer users concrete acknowledgement for their accomplishments (Zichermann & Cunningham, 2011). In cybersecurity training, employees

can accumulate points for completing training modules, earn badges for demonstrating mastery, and achieve leaderboard rankings based on their overall performance.

- **Challenges and Quests:** By articulating learning objectives as challenges or quests, organisations can construct narratives that guide employees throughout their training. This approach improves engagement and can lead to greater retention of information (Sit et al., 2020).
- **Feedback loops:** Regular feedback promotes continuous improvement. In gamified training, employees receive immediate feedback on their performance, which encourages a sense of achievement and promotes a sense of solidarity and the identification of knowledge gaps (Bhashyam et al., 2018).
- **Social interaction:** Providing opportunities for collaboration and competition between employees improves engagement. Social elements, such as discussion forums and collaborative tasks, foster a sense of community and shared responsibility for cybersecurity practices (Harteveld et al., 2016). Storytelling and scenario-based learning: Incorporating narratives or real-world scenarios into training can help employees better relate to the content. Storytelling improves emotional engagement and contextualises vital information in the workplace (McGonigal, 2011).

Different types of cybersecurity awareness games, their effectiveness, and the challenges associated with their implementation will be explored and categorised into simulation games, board games, and digital games, thus discussing their strengths and weaknesses, and the challenges of integrating these games into local governments' training programmes. Cybersecurity awareness games can be categorised into three main types: simulation games, board games, and digital games, described as such:

- (i) **Simulation games:** Simulation games provide realistic scenarios that allow players to experience cybersecurity challenges and decision-making processes firsthand. These games often simulate phishing attacks, data breaches, and incident response scenarios (Anderson et al., 2020). Research indicates that simulation games can significantly enhance players' understanding of cybersecurity risks and their ability to recognise threats (Barker et al., 2019). For instance, the "Phisher's Island" game simulates a

phishing attack environment, helping players identify phishing emails and learn safe online practices (Sätra et al., 2020). However, it is important to design effective simulations that accurately reflect the needs of the participants. Reflecting real-world scenarios can be challenging and may require substantial resource investment (Griffin et al., 2021).

- **Interactive simulations:** Interactive simulations provide real-world scenarios in which employees can exercise their decision-making skills in a secure environment. Tools such as ‘Phishing Simulation’ and ‘Cyber Escape Room’ offer entertaining experiences to raise awareness of cybersecurity.
- **Phishing Simulation Tools:** Platforms like KnowBe4 and Wombat Security allow organisations to conduct simulated phishing campaigns that push employees to recognise potential threats. They can measure how often employees fall victim to phishing attacks and provide tailored training based on the results (KnowBe4, 2021).

(ii) **Board games:** Board games offer a traditional, yet effective approach to improving cybersecurity awareness. These games often involve teamwork, strategy, and critical thinking, solidifying concepts related to cybersecurity while fostering collaboration among players (Krebs et al., 2021). Studies have shown that board games can improve knowledge retention and engagement. Participants gain insight into security practices and terminology in an interactive and relaxed setting (Barker et al., 2019). However, the challenge lies in scaling such games for large organisations and ensuring that they align with varying levels of employee knowledge (Goh et al., 2020).

- **Cyber Escape Room:** This novel tool uses escape room concepts to offer immersive learning experiences in which teams collaborate to solve cybersecurity-related problems within time limits (Ray et al., 2020). Solving these problems requires individuals to apply their knowledge of cybersecurity in an interactive environment.

- **CyberSecure:** This programme combines a quiz format with gamification components, such as points, levels, and awards that users can earn by engaging with material on cybersecurity best practices (CyberSecure, 2021).

(iii) Digital games: Digital games, including serious games and gamified training modules, take advantage of technology to create engaging learning experiences. Serious games are designed specifically for educational purposes, incorporating gameplay mechanics that improve learning outcomes (Gee, 2007). Research by Barlow et al. (2021) suggests that digital games can effectively deliver complex cybersecurity concepts while keeping participants engaged. For example, the "Cybersecurity Lab" game allows users to experience real-world cybersecurity challenges in a controlled environment. However, the user interface and the quality of the design are critical to ensure that participants remain engaged and are not deterred by technical difficulties (Mowers et al., 2020).

- **Learning Management Systems (LMS) with gamification elements:** Modern Learning Management Systems (LMS) often come equipped with gamification features that facilitate engaging training experiences. Platforms such as Moodle and TalentLMS provide organisations with the ability to create customised courses with integrated game mechanics. For example, Moodle as an open-source platform allows educators to create interactive learning environments with features such as badges, achievements, and gamified activities. The use of localised and contextualised scenarios within the Moodle environment can improve the understanding of specific cybersecurity threats relevant to their organisation (Moodle, 2021). And finally, TalentLMS, the platform, enables organisations to create courses that include quizzes, leaderboards, and badges for completed tasks, promoting friendly competition among employees (TalentLMS, 2021).
- **Mobile applications:** With the advent of mobile technology, the adoption of gamified training applications can reach employees anytime, anywhere, improving accessibility. Developers create apps like "Security Awareness" and "CyberSecure" as bite-sized learning experiences that engage users with various gamified aspects.

- **Security Awareness Training:** Offers mobile-friendly modules built primarily for brief and entertaining training bursts, helping to maintain user attention while successfully imparting essential cybersecurity awareness information (Security Awareness Training, 2021).

The findings of the SLR that was conducted to identify key elements, design considerations, and validation methods to develop cybersecurity awareness strategies using gamification. The variety of gamification strategies, intended audiences, design frameworks, validation techniques, and the principal outcomes identified in the 25 PRISMA framework output of relevant studies showed when gamification was used well, government and organisational settings saw significant improvements in how well people followed rules and how safe they were. Table 4.2 summarises the PRISMA outcomes of the gamified cybersecurity awareness strategies.

Table 4-2: Findings table

Gamification Approach	Target Audience	Design Framework	Validation Method	Key Outcomes
Quizzes	Students	Bloom's Taxonomy	Pre- and Post-tests	Improved retention and engagement
Role-playing	Employees	ARCS Model	Surveys	Increased awareness and motivation
Simulation Games	IT Professionals	ADDIE	Behavioural Tracking	Sustained behaviour change
Interactive Storytelling	General Public	Custom Framework	Focus Groups	Enhanced learning experience
Scenario-based Learning	Government Staff	ADDIE	Longitudinal Tracking	Improved policy compliance
Points and Badges	Mixed Audiences	Gamification Design Matrix	Surveys	Higher participation rates
Leaderboards	Students	ARCS Model	Pre- and Post-tests	Competitive engagement
Feedback Loops	Employees	Bloom's Taxonomy	Behavioural Tracking	Reinforced learning outcomes
Simulation-based Training	Government Staff	Custom Framework	Surveys	Improved compliance
Cybersecurity Trivia	General Public	Gamification Design Matrix	Focus Groups	Increased awareness
Role-playing Scenarios	Students	ADDIE	Pre- and Post-tests	Improved retention
Quizzes and Badges	Employees	ARCS Model	Surveys	Motivated learning
Interactive Games	IT Professionals	Bloom's Taxonomy	Behavioural Tracking	Behavioural change
Story-based Learning	General Public	Custom Framework	Focus Groups	Engaging experience
Simulation Exercises	Government Staff	ADDIE	Longitudinal Tracking	Policy adherence
Gamified Modules	Mixed Audiences	Gamification Design Matrix	Surveys	Higher engagement
Leaderboards and Points	Students	ARCS Model	Pre- and Post-tests	Competitive motivation
Feedback Mechanisms	Employees	Bloom's Taxonomy	Behavioural Tracking	Improved outcomes
Scenario Games	Government Staff	Custom Framework	Surveys	Awareness improvement
Trivia Challenges	General Public	Gamification Design Matrix	Focus Groups	Knowledge enhancement
Role-play and Simulation	Students	ADDIE	Pre- and Post-tests	Retention and engagement

Quizzes and Storytelling	Employees	ARCS Model	Surveys	Motivated awareness
Interactive Scenarios	IT Professionals	Bloom's Taxonomy	Behavioural Tracking	Behavioural impact
Narrative Games	General Public	Custom Framework	Focus Groups	Learning enhancement
Simulation and Role-play	Government Staff	ADDIE	Longitudinal Tracking	Compliance improvement

The validation methods for development and usage of cybersecurity awareness strategies using gamification should allow:

- **Engagement through competition:** gameplay fosters active participation and retention, which is crucial in environments where cybersecurity training is often seen as tedious or optional.
- **Microlearning format:** The short and focused nature of the trivia questions aligns well with the time constraints of municipal employees.
- **Immediate feedback:** Real-time responses help reinforce correct behaviour and correct misconceptions instantly.
- **Scalability:** The game can be adapted to different departments and roles within local government structures. To effectively apply the Trivia Twirl model in South Africa, several design adaptations must be considered.
- **Localisation of Content:** Questions should reflect local cybersecurity threats, terminology, and policy frameworks (e.g., POPIA compliance).
- **Language accessibility:** Multilingual support (e.g., Xitsonga, isiZulu, Afrikaans, Sepedi) can improve inclusivity and comprehension. Unfortunately, there still a need to develop a South African language cybersecurity awareness game tool.
- **Cultural Relevance:** Incorporating local analogies, examples, and even indigenous game mechanics (as seen in CyberMoraba) can enhance engagement.
- **Integration with existing platforms:** Embedding the game in municipal e-learning portals or mobile apps can increase accessibility.

4.4 Gamification Tools

There are a multitude of tools and platforms available to implement gamification in cybersecurity awareness training. These tools range in functionality, usability, and adaptability, allowing organisations to select the most appropriate solutions based on their specific needs. Human error remains a critical factor in many successful cyberattacks, underscoring the importance of ongoing employee education (Hadnagy, 2018; Ponemon Institute, 2021).

Table 4-3 represents a high-level summary of cybersecurity games that could be used in a local government setting. The games drawn from the 25 PRISMA literature review studies. Their strengths and weaknesses are highlighting and their relevance to local government setting is set based on the numbering priority.

Table 4-3: Summary of cybersecurity games that could be used in government settings.

Relevance	Game	reference	Strengths	Weaknesses
1.	Cybersecurity Trivia Twirl	Smith et al., (2022)	Encourage active learning through quiz-based participation. Quick to deploy and easy to understand.	May lack depth in covering complex cybersecurity topics. Limited scalability for large organisations.
2.	CyberCIEGE	Cone et al., (2004)	Simulate network security scenarios for practical learning. Comprehensive coverage of varied cybersecurity issues.	Requires technical expertise to effectively use It can be too complicated for beginners without proper guidance.
3.	CyberAware	(Jones & Perez, 2018)	Focusses on real-world cybersecurity threats. Provides targeted exercises for different user roles.	Limited interactivity compared to other gamified solutions May not be appealing to younger audiences due to format.
4.	Threat Defender	Brown & Smith, (2019)	Interactive gaming encourages strategic thinking in threat management. Supports multi-player scenarios for team-based learning.	Requires robust technical infrastructure for seamless operation. High setup and maintenance costs.

Cybersecurity Trivia Twirl was developed by the Centre for Development of Security Excellence (CDSE) as an interactive, gamified learning tool aimed at improving cybersecurity awareness. The game presents users with a series of trivia-style questions that cover key cybersecurity topics such as phishing, password hygiene, data protection, and insider threats. Players receive immediate feedback, accumulate scores, and are encouraged to replay for mastery. Although it was initially designed for a United State government employees, the

Trivia Twirl model offers several transferable elements that are highly relevant to the South African government context, especially local government.

Cybersecurity Trivia Twirl it is a wheel structure that has six segments (Email Safety, Cyber Insider Threat, Password, Smartphone and Tablets, social media, and Your online presents), each representing a different Cybersecurity category (see Figure 2-5).



Figure 4-2: CDSE Cyber Trivia Twirl (Source: CDSE)

You've landed on Cyber Insider Threat.

TAKE THE QUIZ!

Which of these should be considered cyber insider threat?

- SOMEONE WHO INTENTIONALLY RELEASES TOP SECRET INFORMATION VIA COMPUTER OR OTHER ELECTRONIC MEANS
- SOMEONE WHO ACCIDENTALLY DISCLOSES PROTECTED INFORMATION BY STORING IT IN THE "CLOUD"
- SOMEONE WHO COPIES PROTECTED INFORMATION TO A FLASH DRIVE AND GIVES IT TO THE PRESS
- ALL OF THE ABOVE



Which of the following is a best practice when using LinkedIn?

- BE CAREFUL WHAT INFORMATION YOU SHARE ONLINE
- DON'T CLICK ON UNTRUSTED URLS
- KEEP YOUR COMPUTER'S ANTI-VIRUS UP TO DATE
- ALL OF THE ABOVE



Figure 4-3: CDSE Cyber Trivia Twirl Quiz (Source: CDSE)

Figure 4-3 illustrates the CDSE's Cybersecurity-Trivia Twirl. It is known as the cybersecurity SPIN THE WHEEL button game (see Figure 2-5) because it allows the player to spin the wheel until it stops in one of the segments which provide at least five multiple choice questions. The player will then answer the questions. If the player correctly answers three or more questions, that category segment is removed from the wheel and the player may spin the wheel again to play in other segments. If the player incorrectly answers three or more questions, the player is provided a chance to try again or spin the wheel to select another category. Play continues until all six categories have been completed successfully.

Due to its non-complication characteristics as it is an active learning through quiz-based participation game and easily to deploy, the CDSE's Cybersecurity-Trivia Twirl was selected

and randomly tested for the suitability in the municipality context by two CCLM IT employees. In this regard it was used in this study.

4.5 Recommendation

Current research indicates that there are substantial gaps in the application of gamification, especially in the local government of South Africa, even though it offers a promising way to raise cybersecurity awareness. Although studies conducted in South Africa are still small in scope and scale, international research has shown that gamified training can increase engagement and retention. A crucial research and implementation gap is highlighted by the absence of regional frameworks, empirical support, and thoughtful integration into public sector training initiatives.

Cybersecurity awareness games aim to improve participation and knowledge retention by offering interactive and enjoyable training experiences. Although gamification tools show tremendous promise in improving cybersecurity awareness, companies must be aware of the obstacles and factors associated with the implementation of gamified training.

- **Harmonising Engagement with Gravity:** Organisations can face the problem of achieving an optimal balance between engagement and the gravity of cybersecurity training. Although gamified aspects can encourage employees, it is essential to maintain a believable tone and content that underscores the importance of cybersecurity responsibilities (Harteveld et al., 2016).
- **Comprehending individual variations:** Individuals have varying preferences and motivations for learning. Therefore, organisations must tailor gamification components to address the unique demands, interests, and personalities of their employees (Gonzalez et al., 2017). Personalised experience can improve engagement and information retention.
- **Financial limitations:** Creating and executing gamified training programmes may require preliminary expenditures for technology, design, and content creation. Organisations must evaluate available resources and ensure that selected gamification technologies yield a substantial return on investment by markedly improving cybersecurity knowledge and compliance (Higgins et al., 2018).

The effectiveness of cybersecurity awareness games in improving knowledge and changing behaviour is supported by existing research. Games provide an interactive learning strategy that caters to various learning styles, since games can engage visual, auditory, and kinaesthetic learners (Deterding et al., 2011). Studies show that participants in cybersecurity games demonstrate that participants experienced improved threat recognition, increased motivation for learning, and increased cybersecurity awareness compared to traditional training methods (Higgins et al., 2020; Sekaran et al., 2021). Furthermore, the competitive aspect of games can motivate participants to perform better and retain information longer (Dupuis et al., 2021).

Despite their benefits, organisations face several challenges in incorporating cybersecurity awareness games into their training programmes. One primary concern is the resource and time commitment required to develop and implement these games effectively (Griffin et al., 2021). Additionally, it can be daunting to ensure that games align with the objectives of the local government objectives and adequately address specific cybersecurity risks. Organisations should also assess the effectiveness of these games to measure knowledge retention and behaviour change (Barker et al., 2019). Finally, employee engagement can vary, necessitating adaptive strategies to cater to diverse audiences (Krebs et al., 2021).

Research on human factor weaknesses and password management issues has started in South Africa, but not many studies have specifically looked at gamification as a remedy. Furthermore, local governments have limitations that require customised gamification tactics, such as compatibility with low bandwidth, multilingual content, and adherence to federal cybersecurity regulations.

To maximise impact, organisations should:

- enhance game mechanics with clear learning objectives and scenarios in real life,
- monitor performance and performance metrics,
- improve challenge over time, reduce habituation, and maintain curiosity, adjust difficulty levels to different skill sets, and ensure accessibility for all users.

For gamified cybersecurity awareness programmes to be successful and long-lasting, interdisciplinary cooperation, pilot testing, and continuous evaluation will be necessary to close these gaps. By presenting a gamified framework created especially for local governments and influenced by local realities and international best practices, this dissertation helps close that gap. As cyber threats become increasingly complex, gamification becomes a powerful enabler of lasting change. When carefully designed and continuously developed, gamified programmes make employees active defenders, strengthening the resilience of an organisation to attacks that are growing.

4.6 Conclusion

Gamification is a creative and promising strategy for raising awareness of cybersecurity, especially in local government organisations. Gamified training can turn passive learning into active participation using game mechanics, such as challenges, rewards, and real-time feedback. This promotes safer digital behaviour and a deeper understanding of cybersecurity principles.

When carefully implemented, gamification principles can help address the main weaknesses in local government, particularly those associated with human error and social engineering. Although the advantages are obvious, careful planning, the support of stakeholders, and alignment with more comprehensive cybersecurity strategies are necessary for successful implementation. It is necessary to consider and reduce constraints such as scarce resources and disparities in digital literacy by using scalable tools and inclusive design.

Cybersecurity is a critical issue for local governments in South Africa as they strive to protect sensitive information and maintain citizen confidence. Conventional training approaches often fail to adequately engage employees and cultivate a culture of cybersecurity awareness. The implementation of gamification offers a viable approach to improve cybersecurity training, making it more engaging and relevant. Using gamified strategies, local governments can improve employee engagement, increase knowledge retention, and eventually strengthen their cybersecurity posture. South African towns, by implementing gamification in their cybersecurity strategies, can improve the security of the public sector and successfully address modern cyber threats.

In the end, incorporating gamification into cybersecurity awareness campaigns provides a way to develop a public sector that is more knowledgeable and resilient. Local governments can improve their cybersecurity posture and help create a safer online environment for all residents by implementing customised gamification tools and confirming their efficacy with performance metrics and structured feedback. Strong theoretical, legal, and strategic responses are necessary to address the dynamic interplay of vulnerabilities, threats, and attacks that define the South African cybersecurity environment. Despite progress through national frameworks and legislative tools, critical infrastructure and personal data remain vulnerable due to ongoing implementation and awareness gaps. Although cybersecurity theories and frameworks provide useful guidance, their applicability and ongoing development are essential to their efficacy. Gamification offers a fresh and possibly revolutionary way to raise awareness of cybersecurity, especially in local government contexts. Current research shows that despite its potential, there are not enough thorough studies and contextualised applications in South Africa. Closing these gaps with focused, gamified interventions could greatly improve the country's cybersecurity resilience, particularly for public sector employees, who are frequently the first to defend against cyberattacks.

CHAPTER 5

EMPIRICAL FINDINGS

5.1 Introduction

Manpreet (2017) refers to data analysis as the process of inspecting, cleaning, transforming, and modelling data to discover useful information, make suggestions for conclusions, and support decision making. Furthermore, Liamputtong (2009) affirms that different types of data analysis can be used in qualitative research to make sense of the data at hand. That includes, amongst others, thematic analysis, narrative analysis, discourse analysis, and semiotic analysis. However, as described above, thematic data analysis was used. According to Braun and Clarke (2024), thematic analysis (TA) is a set of methods for developing and interpreting patterns of meaning in qualitative data

The aim of this Chapter is to present the work conducted to achieve EO1, EO2 and EO3:

EO1: *“Conduct a brief survey using questionnaires to identify the level of awareness of local government employees.”*

EO2: *“Develop focus groups for local government employees, allowing them to interact with the selected cybersecurity awareness game.”*

EO3: *“Use semi-structured interviews to understand the cybersecurity awareness of local government employees to verify the recommendations formulated from the literature and the interaction with the selected gamification tool.”*

5.2 Focus group Analysis

Table 5-1 and Figure 5-1 illustrate the participants who participated in this study during the focus group and interview process. It shows the distribution of participants by age, gender, occupation, and education level.

Table 5-1: Interview Participants biography

Participants	Age group	Number
Age	18-35	13
	36 – 50	7
	51 +	5
Gender	Male	12
	Female	13
Occupation	Employee	14
	IT professionals	6
	Management	5
Level of education	Diploma	10
	Bachelor's Degree	14
	Honours Degree	1
	Master's Degree and PHD	0

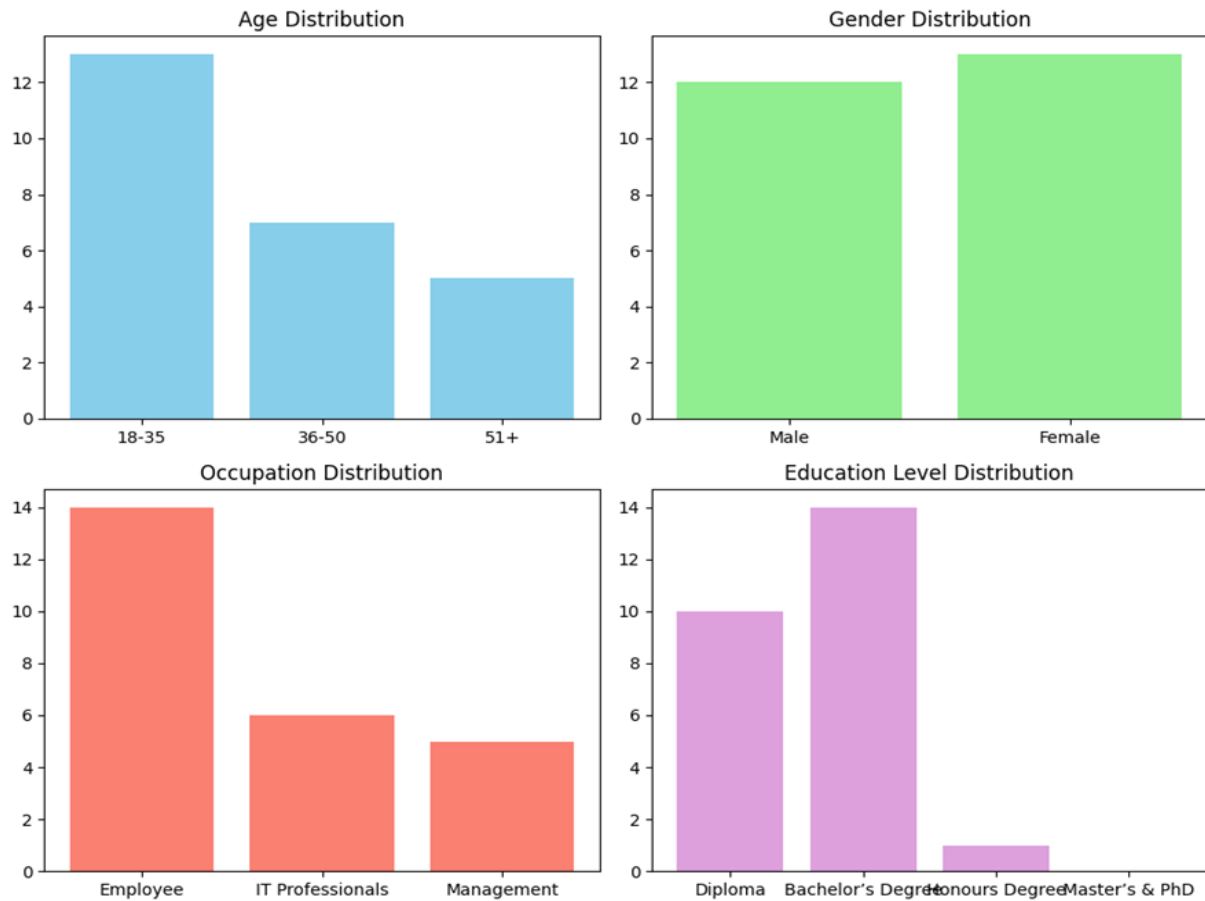


Figure 5-1: Participant demographic distribution.

The number of participants in this study is made up of local government workers, including the management component, IT professionals, and general employees. To present the analysed data, the following codes (see Table 5.2) as pseudonyms were used to preserve the anonymity of the participants, which were maintained throughout this study.

Table 5-2: Participants codes

Code	Description	Code	Description
E1	Employee one	M1	Management one
E2	Employee two	M2	Management two
E3	Employee three	M3	Management three
E4	Employee four	M4	Management four
E5	Employee five	M5	Management five
E6	Employee six	I1	IT one
E7	Employee seven	I2	IT two

E8	Employee eight	I3	IT three
E9	Employee nine	I4	IT four
E10	Employee ten	I5	IT five
E11	Employee eleven	I6	IT six
E12	Employee twelve		
E13	Employee thirteen		
E14	Employee fourteen		

The generated data were transcribed, coded, and arranged into different categories and themes. Furthermore, data were grouped into four categories outlined as cyber security knowledge assessment for employees, IT professionals and management, employees, IT professionals and management emotional response, experiences with the trivia twirl game, attitude toward gamification and implementation, and feedback. In line with the above categories, the themes were developed under each category. Furthermore, the themes that emerged during the analysis of the data are captured and discussed (see Table 5.3).

Table 5-3: Themes

Themes	Theme descriptions
Theme 1	Knowledge of cyber security in local government.
Theme 2	Confidence in cyber security within local governments.
Theme 3	Concepts and areas of cyber security learnt in playing the game.
Theme 4	Applicability of cyber security knowledge in a real-life situation.
Theme 5	Perceptions about cyber security.
Theme 6	Enhancement of cyber security
Theme 7	The capacity of the local government to implement gamification to improve cybersecurity knowledge.

5.3.1 Theme 1: Knowledge of cybersecurity in local government

The theme Knowledge of Cybersecurity in Local Government emerged prominently during the analysis. Participants were asked to self-assess their cybersecurity knowledge before and after participating in the Trivia Twirl game. Before playing the game, employees predominantly rated their knowledge as low to average, while IT professionals rated themselves higher, reflecting their formal training and job responsibilities. Management participants showed a mix of very low and average ratings.

Table 5-4: Cybersecurity knowledge before playing the Trivia Twirl Game

Participants	Very low	Low	Average	High	Very high
Employees	2	5	7	0	0
IT Professionals	0	0	0	2	4
Management	2	0	3	0	0

After playing the game, a significant improvement was observed in all groups (see Table 5.5). The employees shifted from low/average to high/very high ratings. IT professionals maintained high ratings and management participants moved from very low/average to high. This change indicates the effectiveness of the Trivia Twirl game in increasing cybersecurity awareness.

Table 5-5: Cybersecurity knowledge after playing the Trivia Twirl Game

Participants	Very low	Low	Average	High	Very high
Employees	0	0	5	7	2
IT Professionals	0	0	0	0	6
Management	0	0	0	5	0

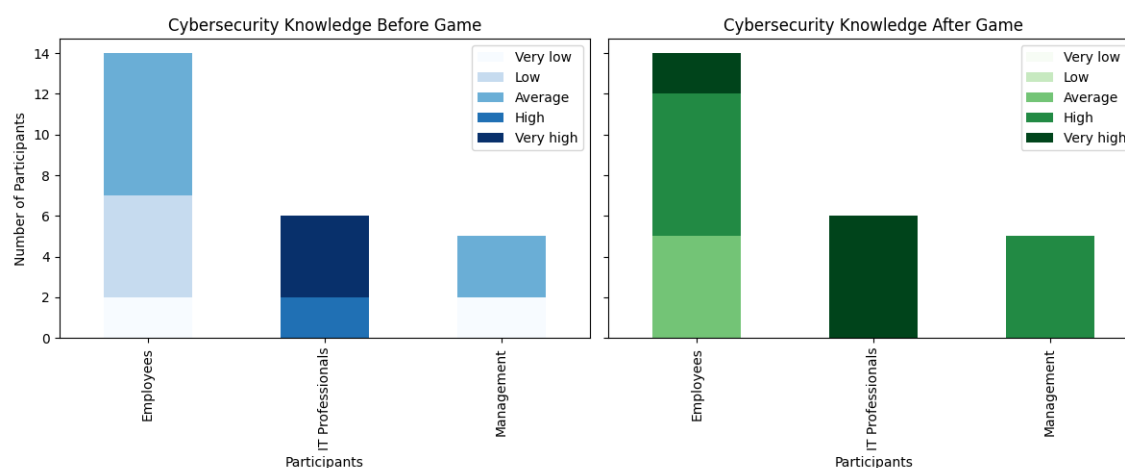


Figure 5-2: Cybersecurity knowledge before and after playing the game

Figure 5.2 illustrates that a gamified learning increases motivation, promotes continuous participation, and fosters a stronger cybersecurity culture within organisations. These findings are corroborated by the literature work which found that employees trained with gamified

methods demonstrated significantly better understanding and application of cybersecurity practices compared to those trained with traditional methods (Urhuogo & Addo, 2024).

5.3.2 Theme 2: Confidence around cybersecurity within local governments

The theme 'Confidence around cybersecurity within local governments', illustrated in Table 5.6, highlights a significant shift in participant confidence levels before and after engaging with the Trivia Twirl game. Initially, only IT professionals showed extreme confidence, while employees and management showed moderate to low levels of confidence. This disparity is attributed to prior training and daily exposure to cybersecurity issues.

Table 5-6: Confidence Before Playing Trivia Twirl

Participants	Not confident at all	Slightly confident	Moderate confident	Very confident	Extremely confident
Employees	4	10	0	0	0
IT Professionals	0	0	0	6	0
Management	0	0	5	0	0

After playing the game, a marked improvement was observed in all groups (see Table 5.7 and Figure 5.3). Employees and management reported an increase in confidence, and many moving from low to moderate or high confidence levels. This improvement is likely due to the interactive and engaging nature of the game, which effectively introduced cybersecurity concepts in a digestible format.

Table 5-7: Confidence After Playing Trivia Twirl

Participants	Not confident at all	Slightly confident	Moderate confident	Very confident	Extremely confident
Employees	0	0	3	8	3
IT Professionals	0	0	0	0	6
Management	0	0	2	3	0

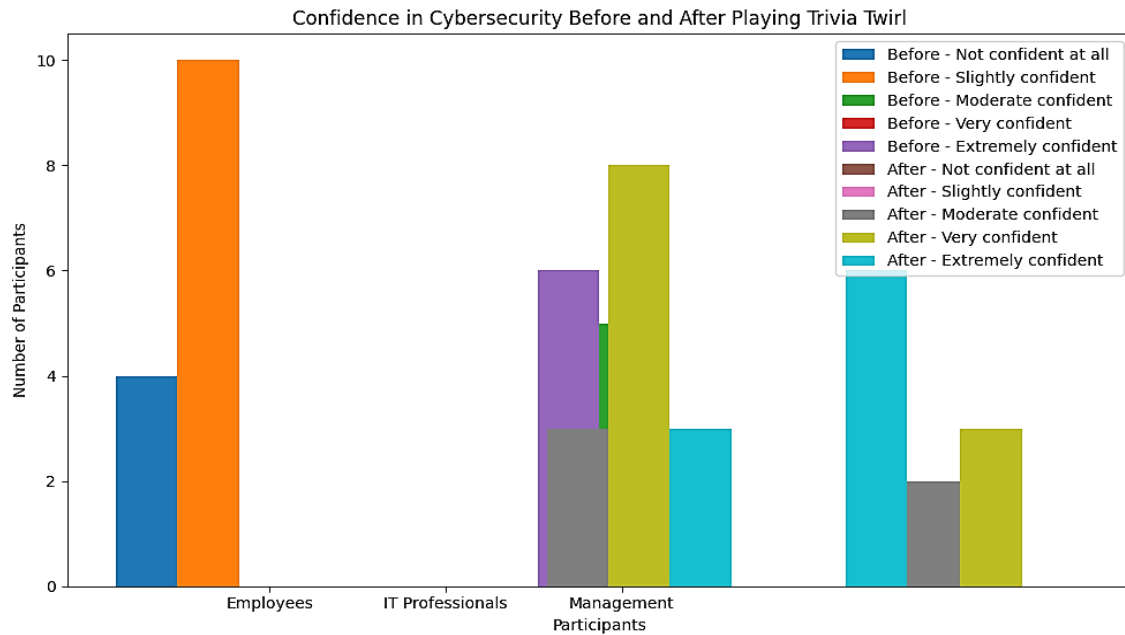


Figure 5-3: Confidence in Cybersecurity Before and After Playing Trivia Twirl

These findings are supported by Urhuogo and Addo (2024) who argue that gamified training increases employee engagement, promotes continuous learning, and fosters a proactive cybersecurity culture. Their study confirms that gamification not only enhances knowledge but also builds confidence in identifying and responding to cybersecurity threats. Overall, the Trivia Twirl game proved to be a valuable tool for raising confidence in cybersecurity among local government employees, management, and IT professionals.

5.3.3 Theme 3: Concepts and areas of cybersecurity learnt in playing the game

This section explores the theme 'Concepts and areas of cybersecurity learnt in playing the game'. The analysis highlights how the participants' understanding of cybersecurity concepts evolved through the gamified learning experience. Table 18 shows the understanding of cybersecurity concepts and areas by employees, IT professionals, and management before playing the game.

Table 5-8: Understanding Before Playing the Game

Participants	Phishing	Password Security	Malware	Data Protection	Safe Internet Practices
Employees		√	√		
IT Professionals	√	√	√	√	
Management		√			√

Before playing the game, employees only understood password security and malware as concepts and areas of cybersecurity, while management only understood password security and safe practices, and IT professionals as owners of the territory understood phishing, password hacking, malware, and data protection. However, after playing the game, all participants made a very significant improvement in understanding the concepts and areas of all participants. This is evident in the table depicted below. Therefore, the employees understood the concepts of phishing, password security, malware, and safe Internet practices. Meanwhile, management understood phishing, password security, data protection, and safe Internet, and IT professionals took the lead by understanding all concepts and areas of cybersecurity.

Table 5-9: Understanding After Playing the Game

Participants	Phishing	Password Security	Malware	Data Protection	Safe Internet Practices
Employees	√	√	√		√
IT Professionals	√	√	√	√	√
Management	√	√		√	√

5.3.4 Theme 4: Applicability of cybersecurity knowledge in real-life situations

The applicability of cybersecurity knowledge in real-life situations emerged as a significant theme during data analysis. Participants in all roles, including employees, IT professionals, and management, expressed that the knowledge gained from playing the Trivia Twirl game was not only relevant to their work, but also applicable to their personal digital lives. This consensus reflects the growing importance of cybersecurity awareness in the digital age, where people are increasingly exposed to cyber threats, such as phishing and malware.

Table 5-10: Participant ratings on Applicability of Cybersecurity Knowledge

Participants	Not likely	Slightly likely	Moderately likely	Very likely	Extremely likely
Employees	0	0	0	6	8
IT Professionals	0	0	0	0	6
Management	0	0	0	0	5

In Table 5.10, it is quite clear that local government employees participated in this study and have almost reached a consensus around the view that the cybersecurity knowledge learnt through gamification is applicable in real-life situations. The reason for this convergence is maybe because most people are largely in cyberspaces and they are being victimised by different cybersecurity threats such as malicious attacks, phishing, just to list a few, because of a lack of knowledge of cyber security. Therefore, after playing the game, the participants felt that the cybersecurity knowledge they had learnt was highly applicable in the real-world situation.

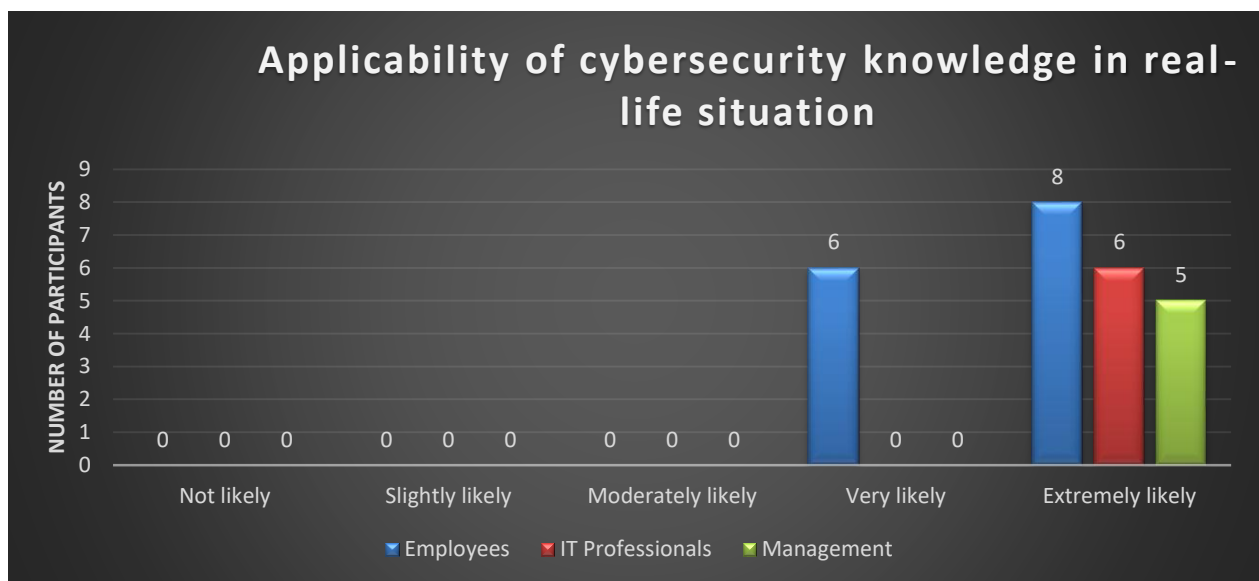


Figure 5-4: Applicability of cybersecurity knowledge in real-life situations

To support this finding, SECNORA (2025) reported that gamified cybersecurity training significantly improves the application of real-world knowledge, allowing users to better avoid phishing scams and adopt safe practices. Similarly, MoldStud Research (2024) emphasised that gamified training improves critical thinking and decision-making, preparing learners to apply cybersecurity knowledge effectively in everyday scenarios.

5.3 Interviews

5.4.1 Theme 5: Perceptions about cybersecurity knowledge

Several questions were asked during the interviews with the participants from the different municipality positions. Participant M4 who is in a management position, raised the following:

Exhibit 1: *Knowledge of cyber security is of paramount importance in the local government, as it helps us better understand concepts and areas of cybersecurity such as cloning, social engineering, social hacking, and insider threats.*

Exhibit 2: *My understanding of cybersecurity has expanded significantly as a result of playing this game, particularly regarding the methods by which social engineering techniques, such as hacking, ransomware, and phishing, are carried out. I am very grateful for this discovery.*

Exhibit 1 shows that the result of this participant expression is that he has learnt quite a lot about cyber concepts and its areas through playing the game. Moreover, M5 in Exhibit 2 vowed in favour of the M4. In Exhibit 2, M5 highlights the important role that the game is playing in expanding the cyber knowledge amongst the local government employees. Meanwhile, on the other hand, I4, who is an IT professional, had the following to say in support of the M4 and M5 views as illustrated by exhibit 3 to 5.

Exhibit 3: *I have learnt about social hackers and how they operate, as well as ways in which they can be avoided in a local government. The trivia twirl game has also taught me about the severe consequences of unsafe practices in cyberspaces.*

Exhibit 4: *When playing the Trivia Twirl game, I have learnt a lot about whaling, frequent change of passwords, and safe practices around cyberspaces, which I did not know before playing the game.*

Exhibit 5: *Since I started working in local government many years ago, I have never had the opportunity to learn about cybersecurity threats in such a straightforward manner. I have gained a lot of knowledge that I believe is important for my safety and the safety of the local government.*

The viewpoint driven by this participant turns out to be in full support of the above-raised point of view. However, this one stress much on social hackers as an area within cybersecurity within which the prevention and the possible consequences are learnt in playing the game. On the other hand, exhibit 4 illustrates the feedback from E5's interview. which indicated it is unequivocal that the trivia twirl game is a significant tool for teaching cyber security to the incumbents of the local government.

Kim et al. (2025) found that gamification significantly improves the understanding of cybersecurity concepts by learners. Huitema and Wong (2025) emphasised that gamification bridges educational gaps by making complex cybersecurity topics more accessible and engaging. The feedback from the interviews as indicated in Exhibit 1 to 5 corroborate with the researcher's observation and the literature work by Kim et al. (2025) and Huitema and Wong (2025). The findings illustrate the converges of the viewpoints showing the observation of the researcher that the trivia twist not only refreshed the minds of the participants but was also able to teach and leverage their understanding of cybersecurity.

Exhibit 6: *“Based on the dangers that I saw when playing the trivia twirl game, we really need to protect our information whenever we go online through cybersecurity” said E2.*

Before playing the Trivia Twirl game, many participants had negative or indifferent perceptions about cybersecurity. However, after playing the game, their perceptions shifted significantly toward a more positive and proactive approach. The game helped participants understand the importance of cybersecurity in protecting personal and organisational

Exhibit 7: I1 mentioned that *“Playing the game has broadened my understanding of cyber security, particularly with regard to the extent to which cyber security can help protect personal information of employees and that of the organisation in the local government”*.

information. Exhibit 6 illustrates that after playing the game a positive perception about cyber security knowledge rise because the game has taught E2 the importance of protecting information through cyber security. The latter was supported by I1 in Exhibit 7. The insight highlighted by this respondent is that the trivia twirl game played a very significant role in demonstrating the importance of cyber security in protecting information within the local government. Furthermore, another perspective has been noted from M3, who said that:

The result from the point of view of M3 show that trivia twirl game has made realisation how important it is to protect personal and workplace information using cybersecurity when using Internet devices. This turns out to be in support of the other points of view raised by the participants and ultimately confirms the researcher’s observation that the trivia twirl game has

Exhibit 8: *From now on, I will be very careful and cautious when navigating the Internet platforms using technological devices both at work and at home to maximise the safety of my personal and work information.*

completely changed perceptions about cybersecurity threats. This could be because these participants serve in the same local government and have never received cyber security before; therefore, they have never understood how important cyber knowledge is in terms of protecting information.

Donekal et al. (2024) developed a gamified training framework using extended reality (XR) and Generative AI to simulate real-time cyberattack scenarios. Their study found that immersive gamified environments significantly improve user perceptions of cybersecurity by making threats more tangible and relatable. As illustrated by exhibits 7 to 9, participants

reported a greater appreciation for the role of cybersecurity in protecting personal and organisational data.

Exhibits 1 to 9 emphasised that gamification improves learner engagement and positively shifts attitudes toward cybersecurity (Marciano, et al., 2024). Furthermore, clearly, participants initially viewed cybersecurity as abstract or irrelevant and they begin to develop a more proactive and informed mind set after participating in gamified training modules.

5.4.2 Theme 6: Enhancement of cybersecurity understanding

Urhuogo and Addo (2024) propose a comprehensive gamification model designed to improve cybersecurity resilience in organisations. Their study emphasises that gamified training fosters deep understanding, proactive threat mitigation, and resilient cyber culture. The model includes simulation scenarios and reward systems that significantly improve knowledge retention and application. Similarly, Donekal et al. (2024) developed a gamified platform using extended reality (XR) and Generative AI to simulate real-time cyber threats. Their findings show that immersive gamified environments lead to greater user engagement and improved understanding of cybersecurity threats and responses.

Exhibit 10: E1 mentioned that: *"I support the use of the trivia twirl game as a method to improve cybersecurity in local government because it attracts a lot of attention and gains knowledge faster than reading case studies and compulsory courses for all administrative staff."*

E6 said: *"I recommend the use of the trivia twirl game as a method to improve cyber security knowledge within local governments for the safety of employees and local government."*

The interview revealed that the Trivia Twirl game significantly contributed to improving participants' understanding of cybersecurity concepts and practices. This is evidenced by the following responses as illustrated by exhibits 10 to 11. The responses of the participants indicate a strong consensus that the Trivia Twirl game is an effective tool to improve cybersecurity understanding. The employees found the game more engaging and informative

than traditional training methods. IT professionals and management echoed this sentiment, highlighting the game's potential to address prevalent cybersecurity threats and recommending its integration into policy and training programmes.

5.4.3 Theme 7: Capacity of the local government to implement gamification to improve cybersecurity knowledge

Although gamification is perceived as an effective method, participants expressed concerns about the readiness of their local government to support such an initiative due to resource constraints. The following participants had the following to say:

Exhibit 12: E7 (Employee): *“I am convinced that if the trivia twirl game can be implemented in our local government, we will learn a lot about cybersecurity and can protect ourselves through cybersecurity. However, our local government is still in a crawling stage in terms of finances, where a lack of ICT resources, poor networks, and IT personnel are the most pressing challenges within our local government.*

I4 (IT Professional): *“The trivia twirl game is very fantastic and could capacitate players with cybersecurity knowledge, and I must inform you that as an IT professional, there are many new things that I didn't know about cybersecurity because technology changes over time. However, enforcing the trivia twirl game as a strategy for the local government to enhance cybersecurity knowledge may require new policies or refinement of policies of operations within the local government; it may also require advanced technologies, which the local government may not be able to provide immediately because they must first be budgeted for and approved by the relevant designated authority.*

M1 (Management): *“With respect to the implementation of the Trivia Twirl game, it needs a stable network and reliable electricity, and now we are still operating under the pressure of load shedding and load reduction. Moreover, as a local government in terms of technological resources and IT personnel.*

The responses from employees, IT professionals, and management reveal a shared enthusiasm for gamification as a tool to improve cybersecurity knowledge. However, they also highlight

significant obstacles to implementation, including financial constraints, lack of ICT infrastructure, and insufficient human resources. These concerns reflect a realistic understanding of the operational limitations within local government entities.

Again, eScribe Meetings (2025) emphasises that while gamified cybersecurity training is effective, many local governments face challenges in implementation due to limited financial resources, inadequate ICT infrastructure, and lack of leadership support. Similarly, Government Technology (2025) notes that human error and under-resourced systems are persistent vulnerabilities in local governments, and that stable infrastructure and policy frameworks are essential for successful cybersecurity programmes.

5.4 Recommendations

The theoretical framework served as a foundational lens through which the data was interpreted and organised throughout the analysis process. By laying a well-established framework, such as the Technology Acceptance Model (TAM) (Davis, 1989) and the Theory of Planned Behaviour (TPB) (Ajzen, 1991), this study provided a structured approach to understanding how participants perceived, engaged with, and responded to gamified cybersecurity training. This framework helped identify key constructs such as perceived usefulness, ease of use, motivation, and behavioural intention, which were instrumental in categorising and interpreting participant responses across themes such as knowledge acquisition, confidence, and applicability. In addition, the theoretical framework guided the development of themes by aligning experiences with theoretical constructs. For example, evolving perceptions and the increase in confidence in cybersecurity knowledge were not only observed, but also contextualised within the dimensions of the framework. This ensured that the analysis remained focused, coherent, and theoretically sound, allowing deeper insights into how gamification influences cybersecurity awareness in a local government context. Ultimately, the framework improved the credibility and analytical depth of the study by linking empirical findings to broader theoretical understandings (Venkatesh & Davis, 2000).

5.5 Conclusion

This Chapter presented a comprehensive analysis of the data collected from local government employees, IT professionals, and management regarding their knowledge and experiences with the Trivia Twirl game. Thematic analysis revealed significant improvements in the understanding, confidence and perceptions of cybersecurity by participants after their participation in the gamified training tool. Themes such as knowledge acquisition, emotional response, and applicability of cybersecurity concepts in real-life scenarios were consistently supported by participant feedback and aligned with existing literature (Urhuogo & Addo, 2024; Kim, Zhong, and Liu, 2025).

The findings also highlighted the transformative potential of gamification in the promotion of culture within the local government. Participants expressed increased motivation and participation, and many advocated for the integration of gamified learning into policy and training frameworks. However, challenges such as limited resources, infrastructure constraints, and policy readiness were identified as barriers to implementation. These insights underscore the importance of strategic planning and investment in ICT to support effective cybersecurity education (eScribe Meetings, 2025; Government Technology, 2025). In general, the results affirm that gamification, when implemented with care, can serve as a powerful tool to improve cybersecurity awareness and resilience in public sector environments.

CHAPTER 6

CONTRIBUTIONS

6.1 Introduction

This Chapter presents the key recommendations derived from the findings discussed in this dissertation and outlines them as contributions of this study to theory, practice, and future research. The recommendations aim to improve awareness of cybersecurity and resilience in local government through the strategic use of gamification. In this regard, this Chapter presents this study's contributions by providing list of recommendations for cybersecurity awareness for the South African local government using a gamification approach. It aims to achieves TO3 and EO4 and the primary objectives and the aim of this study.

6.2 Recommendation 1: Multilayered defence approach

To defend South African local government institutions against increasingly complex cyberthreats, a multilayered cybersecurity defence strategy is necessary. The most crucial, yet most vulnerable element is still LoD 1: people, which requires constant awareness and training to prevent social engineering techniques. Critical infrastructure is protected by LoD 2: technological safeguards, but these must be updated frequently and incorporated with more comprehensive security policies. LoD 4: legal enforcement anchors cybersecurity efforts within a strong regulatory framework, while LoD 3: policy adherence ensures that internal governance promotes secure behaviour and compliance. The Cybercrimes Act and POPIA, two of South Africa's cybersecurity laws, provide strong instruments for accountability and investigation, but their efficacy hinges on inter-agency cooperation and consistent application. South African local governments can create a robust cybersecurity posture that protects public assets, ensures service continuity, and promotes confidence in digital governance by fortifying each line of defence and making sure that they work together.

6.2.1 Layer 1: First Line-of-Defence (LoD 1)

The LoD 1 focus on people who are essential in identifying and thwarting cybersecurity attacks.

- **Recommendation 1.1:** It is recommended that the local government should use gamification to create awareness for employees to know, understand and have techniques of dealing with cybersecurity attacks, social engineering threats, phishing, etc.
- **Risk:** Failure to adherence by the employees will create loopholes for cyber-attacks that could come through their negligence and destroy the organisation.
- **Mitigation:** For example, CCLM should create daily broadcast communication for people to be aware of phishing. These could be achieved by sending internal phishing messages to identify those loophole employees and request them to use the game to train more.

6.2.2 Layer 2: Second Line-of-Defence (LoD 2)

The LoD 2 is classified as a technological safeguard and comprises the following: firewalls that serve as barriers between trusted and untrusted networks, intrusion detection systems (IDS).

- **Recommendation 1.2:** It is recommended that local government's technological infrastructure should always be monitored against anomalous behaviour within the network traffic. Technological safeguarding and defences should include the instruments and methods established to protect local governments' assets and ensure their security against cyberattacks.
- **Risk:** If the organisation fails to obtain and protect its digital infrastructure by allowing any form of attack, this will threaten the organisation.
- **Mitigation:** The CCLM should invest in real-time information on system vulnerabilities that can react autonomously to identified threats to minimise possible harm. The encryption that protects sensitive information during transmission and storage, and access control measures that guarantee that only authorised personnel can access essential systems and data.

6.2.3 Layer: Third Line-of-Defence (LoD 3)

The LoD 3 ensures compliance and guarantees that organisations comply with applicable rules and regulations, mitigating risks related to penalties and harming their reputation.

- **Recommendation 1.3:** It is recommended that local government should implement and maintain policies to cultivate a successful cybersecurity culture. Policies must encompass all aspects of cybersecurity, including incident response, data management, and employee obligations.
- **Risk:** Failure to adhere to cybersecurity policies and frameworks might jeopardise the local government cybersecurity defences.
- **Mitigation:** The CCLM should provide a well-defined policy framework that helps mitigate and reduce risks related to cybersecurity incidents. It should ensure that all personnel understand their responsibilities in ensuring cybersecurity regulations. Furthermore, the internal cybersecurity policies and procedures within local government will ensure that governance frameworks encourage safe practices.

6.3 Recommendation: South African regulatory framework

The cybersecurity landscape in South Africa is governed by several laws and regulations intended to promote secure online activity, such as the Cybercrimes Act, which creates offences for cyber-related crimes, and the Protection of Personal Information Act (POPIA), which ensures the protection of personal data. Compliance with these regulations is essential for organisations to operate legally and ethically in the cyber realm (Kumar & Singhal, 2020). Despite the presence of strict cyberlaws, local governments often face compliance challenges due to resource deficiencies, inadequate awareness, and knowledge disparities (Kok, 2020).

- **Recommendation:** The local government should apply and enforce the South African cyber laws, such as the Cybercrimes Act, POPIA, ECTA, and RICA, which together constitute the legal foundation of the nation's cybersecurity regime, at all its LoDs.
- **Risk:** Failure to adhere to cybersecurity laws will lead to fragmented and isolated cybersecurity protection that will rely on individual employees' knowledge of either protecting the local government network or exposure in handling cybersecurity attacks such as phishing and social engineering.

- **Mitigation:** The CCLM should provide a well-described cybersecurity regulatory law that draws from the main South African cyber laws as highlighted above. The laws should be described in a physical, administrative, and technical format such that they could enable different levels of preventive, detective, corrective, directive, deterrent, and compensating measures. For example, creating a compensating measure could be notifying the employees that some token of appreciation will be provided to an employee that does not put their guard down when coming to cyber-threats and attacks. The latter could increase awareness and education of employees on cybersecurity issues as they will have something to look towards.

6.4 Recommendation: Third-party monitoring

Third-party vendors are crucial for local governments to keep services running, but they also bring real cybersecurity risks because they often have access to internal systems and sensitive data. If this access is not properly monitored, the consequences can be serious: financial losses, service disruptions, and even loss of public trust.

- **Recommendation:** Local governments should monitor third-party access to internal systems, implement zero trust architecture and endpoint detection, conduct comprehensive cybersecurity assessments of all vendors to include cybersecurity provisions in procurement contracts, and collaborate with national cybersecurity agencies for threat intelligence to reduce the supply chain's cyber risks.
- **Risk:** Lack of monitoring cybersecurity attacks could lead to:
 - **Financial loss:** Many cyberattacks against local governments are motivated primarily by financial gain, as hackers exploit weaknesses to demand ransom or steal data (KPMG, 2021). Cyber-attacks have had a significant impact on the economy. Funds from essential public services should be diverted for incident response, recovery, and system improvement (Parker, 2020). According to estimates from the Johannesburg, ransomware attack recovery cost more than R30 million (Nkosi, 2020). These financial

problems are further exacerbated by the possibility of lawsuits by individuals and companies affected by service interruptions (Banda, 2021).

- **Undermining Political justifications:** Cyberattacks may be motivated by politics, seek to undermine public confidence, or interfere with government functions (Dlamini, 2021).
- **Operational disruption:** Some attacks aim to protest by interfering with government services or to draw attention to structural problems in public management (Pillay, 2022). For example, local governments may find it extremely difficult to perform their duties due to cyber incidents. Attacks that compromise data accessibility or reliability can prevent local governments from performing critical functions such as emergency response, water supply, and waste management (Ngcobo, 2021). At the beginning of 2020, Tshwane had problems with its billing system due to a ransomware attack. This led to delays in payment and public dissatisfaction with service delivery (Tshwane Times, 2020).
- **Mitigation:** The CCLM should establish governance structures, train staff, and implement technical controls to transform its monitoring of third-party access to internal systems into actionable cybersecurity measures. For example, the involvement of local stakeholders through awareness campaigns and incident reporting mechanisms ensures that policies reflect the realities on the ground (Generis Online 2024).

6.5 Recommendations for formulating a cybersecurity awareness strategy through gamification

To have a resilient digital environment, cybersecurity best practices are crucial. Despite implementation obstacles, such as cultural resistance and resource limitations, strategic awareness campaigns can greatly improve cyber readiness. With its dynamic and interactive learning experiences, gamification shows promise as a tool to close the gap between technical expertise and user engagement.

- **Recommendation:** Local governments can foster a proactive cybersecurity culture by using customised tactics and integrating verified components. To effectively implement and maximise the gamified cybersecurity awareness tactics, local governments must consider the following recommendations.

- Create a clear framework: Develop a systematic framework that includes explicit objectives, defined target audiences, and appropriate gamification strategies. A well-defined roadmap ensures that all stakeholders understand the desired results and techniques, fostering consistency during the implementation process.
- Leverage technology: Using technology that enables gamified experiences, such as mobile applications or internet platforms, to distribute training information. These solutions improve accessibility and participation in learning for employees, allowing participation at any time and from any location (Davis et al., 2020).
- Cultivate a culture of learning and improvement: Fostering a culture that promotes continuous learning and improvement could increase the adoption of gamified strategies. Encourage transparent dialogue on cybersecurity protocols and offer frequent opportunities for employees to improve and update their knowledge (O'Connor, 2019).
- Incorporate real-world scenarios: Incorporating real-world scenarios into gamified training allows employees to connect their learning with realistic problems they may face. Simulated scenarios that replicate genuine cyber risks can equip employees to respond with a strong response to security issues at work (Hahnagy, 2018).
- Collaborate with stakeholders: Collaborating with various stakeholders, such as cybersecurity experts, educators, and industry professionals, can improve the quality and pertinence of gamified training materials. Engaging with specialists ensures that training aligns with current best practices and alleviates developing threats.
- Evaluate and adjust regularly: A consistent assessment of gamified training programmes is essential to understand their efficacy and pertinence. Organisations must use continuous evaluation techniques, feedback systems, and behavioural metrics to pinpoint areas for improvement and adapt strategies accordingly (James, 2016).
- Incorporate gamification into current training programmes: Organisations must look for opportunities to include gamification in their existing cybersecurity training programmes. Incorporating game components into current content can improve engagement without necessitating a complete review of the training curriculum (Hollis et al., 2018).
- Foster collaboration and team participation: Encourage team-orientated challenges, and collaborative efforts can improve the sense of community and responsibility among

employees. Collaborative activities promote communication, problem solving, and collective learning experiences relevant to cybersecurity (Vance et al., 2021).

- Consistently review and renew content: Cybersecurity risks are constantly evolving, which requires frequent review of training materials to incorporate the most current trends and optimal practices. Using a step-by-step approach allows companies to change their gamified strategies based on changing needs and user feedback (Fischer, 2020).
 - Evaluate the results and modify accordingly: Organisations must implement key performance indicators (KPIs) to assess the effectiveness of their gamified awareness efforts. Continuous evaluation allows companies to pinpoint areas for improvement and modify their methods to more effectively achieve their objectives (Bada et al., 2019).
 - Foster a culture of cybersecurity awareness: Establishing a culture that emphasises cybersecurity awareness is crucial for the long-term effectiveness of any plan. Such results can be achieved by endorsement by leaders, consistent communication on cybersecurity issues, and encouraging a sense of duty among all workers to protect information assets (ISACA, 2021).
- **Risk:** failure to adhere to establishing the gamified strategy as recommended then the organisation will fail to achieve first-hand information that could be used to target the organisation.
 - **Mitigation:** The CCLM could validate the gamified strategy awareness strategy through assessing the efficacy of gamified cybersecurity awareness programmes and collect feedback (James, 2016). These could be done as follows:
 - Pre- and Post-Assessment: The use of pre- and post-assessments is a great method to assess the acquisition of knowledge derived from the gamified strategy. Evaluations must encompass the main topics addressed in training, allowing organisations to compare knowledge levels before and after engaging in gamified activities (Ford, 2014).
 - Surveys and feedback forms: Feedback forms and surveys can provide information on participation and information on gamified training for participants. Organisations can use these tools to collect feedback on the content, delivery and overall experience of

the gamified strategy. Analysing this feedback will facilitate the identification of strengths and opportunities for improvement (Kim & Gilman, 2016).

- Behaviour metrics: Behaviour metrics, including incident reports and phishing simulation scores, could indicate the overall security status of an organisation. Monitoring these measures before and after the implementation of gamified tactics can provide significant insight into their effects on employee behaviour and awareness (Kaplan, 2017).
- Focus groups and interviews: Focus groups and interviews can offer qualitative opinions on the efficacy of the gamified strategy. Interacting with participants enables organisations to explore human experience more thoroughly and obtain subtle insights that surveys may overlook (Baker, 2019). This qualitative methodology improves the evaluation process.

6.6 Recommendations for a good cybersecurity awareness game relevant for the local government setting

Practical cybersecurity training for the local government employees has been found in this study to be relevant and improving interest and engagement. In this regard, it is recommended that:

- **Recommendations:** Local government should integrate gamified training into their cybersecurity awareness programmes. Based on the positive impact of the Trivia Twirl game, local governments should adopt gamified tools such as Cyber-Trivia Twirl as part of their regular training to improve engagement and retention (Urhuogo & Addo, 2024).
- **Risk:** the gamified awareness strategy might not be effective in a poor or lack of internet connectivity environment and an environment that has lack proficient facilitators.
- **Mitigation:** CCLM should addressing challenges such as poor internet connectivity (by providing access to staff, even if they are at home), limited devices, and load shedding is essential for successful implementation. Training and equipping of facilitators that comes from different CCLM divisions will help to break the stigma of cybersecurity being an IT problem.

6.7 Recommendations for an implementation strategy of a good cybersecurity awareness game relevant for the local government setting

The strategic decisions should be taken and provided as directive for implementing gamified cybersecurity awareness programmes. To achieve the latter, it is recommended that:

- **Recommendations:** Local governments should create or revise policies to support the integration of gamification into employee development programmes (Marciano et al., 2024).
- **Risk:** lack of stakeholder engagement such as the involvement of management, IT professionals, and employees in the design and implementation of gamified tools to ensure relevance and acceptance should be avoided at all costs as the municipality might deploy a none accepted technology.
- **Mitigation:** to rollout the cybersecurity programme the policy should provide a space for pilot programmes that start with small-scale pilot implementations of gamified training to assess feasibility and refine the approach before scaling. For example, this dissertation has been developed from the findings such a programme.

6.8 Recommendations for Lack of knowledge on cyber threats

There was a lack of knowledge about cyber problems, making it difficult to obtain relevant data. In this regard, it is recommended that:

- **Recommendations:** The local government should embed through the IT implementation strategy the understanding of cyber concepts such as cyber security threats, Trojan, phishing, ransomware, inappropriate content, and others emerged as one of the most difficult challenges in digital environment.
- **Risks:** Lack of knowledge among the participants could result in a loss of confidence and uncertainty when employees are faced with cybersecurity threats.
- **Mitigation:** as the IT implementation strategy is being rolled out the cybersecurity training facilitators should create posters that could be placed at CCLM corridors and walkways.

6.9 Conclusion

In conclusion, Table 6-1 provide a consolidated literature and empirical recommendations for cybersecurity awareness using a gamification approach aligning them for CCLM.

Table 6-1: Summary of recommendations in alignment to the objectives.

Objective	Findings	Recommendations for CCLM
To explore the literature on different cybersecurity awareness strategies, frameworks, and best practices to identify key elements, design considerations, and validation methods for the development of cybersecurity awareness strategies using gamification.	• Research provides actionable information for CCLM as they look at improving the cybersecurity culture. It highlights the potential of gamification to overcome training fatigue and increase participation in cybersecurity programmes (Donekal et al., 2024). • The literature also shows that validation methods such as pre and post-training assessments and behavioural observations are essential to measure effectiveness (Wang et al., 2016).	• Cyber Trivia-Twirl should be adopted as part of the cybersecurity awareness training. • Include validation methods such as quizzes and feedback surveys to measure impact.
To explore the literature on the gamification tools and techniques that can be used to increase awareness of cybersecurity. Then identify and select cybersecurity games that are suitable for the specific context of the cybersecurity awareness context.	• Gamification tools such as points, badges, leaderboards, and storytelling improve engagement and retention (Deterding et al., 2011; Whitton, 2014). • Serious games tailored to local government contexts are more effective than generic solutions.	• Develop or adapt a gamified training tool that incorporates points, badges, and narrative elements relevant to local government operations.
Conduct a brief survey using questionnaires to identify the level of awareness of local government employees.	• The results indicated low confidence and limited knowledge of cybersecurity among employees, with	• Use survey insights to tailor training content to address knowledge gaps. Continue using focus

Develop focus groups for local government employees, allowing them to interact with the selected cybersecurity awareness game.	misconceptions about phishing and password management. • Focus groups showed greater engagement when using gamified tools.	groups for iterative improvement of gamified training.
Use semi-structured interviews to understand the cybersecurity awareness of local government employees to verify the recommendations formulated from the literature and the interaction with the selected gamification tool.	• The interviews revealed positive perceptions of gamification and its potential to improve cybersecurity understanding. The employees expressed willingness to adopt gamified training if supported by the leadership and integrated into daily work routines.	• Secure leadership support for gamified training initiatives. • Incorporate gamification into regular awareness campaigns and policy frameworks.

CHAPTER 7

Lesson Learnt

7.1 Introduction

This Chapter reflects the lessons learnt during the research process, focusing on both practical and methodological experiences. It examines the challenges faced during the literature review and data collection phases and highlights how these challenges created opportunities for improvement. Understanding these lessons is important because it shows the researcher's ability to adapt, maintain credibility, and ensure that the study meets ethical and methodological standards. Booth, Sutton and Papaioannou (2016) stated that reviewing the literature requires careful planning and critical evaluation, which can be complex and time-consuming. By sharing these experiences, this Chapter aims to provide transparency and offer insights that can guide future research.

7.2 Challenges and opportunities encountered during literature review

The literature review is a critical foundation for any research study. It shapes the theoretical framework, highlights existing gaps, and informs the overall research design. Despite its importance, the process often comes with challenges that require careful planning and strategic solutions. As Booth, Sutton and Papaioannou (2016) note, conducting a systematic literature review involves rigorous planning, critical evaluation, and synthesising diverse sources—tasks that can be both time-consuming and complex. In this study, several challenges emerged during the literature review phase, each of which presented opportunities for growth and refinement. These are outlined in Table 7-1.

Table 7-1: Summary of recommendations in alignment to the objectives.

Challenges	Description of Challenge	Opportunities	Recommendations
Overabundance of Global Literature	Filtering through vast amounts of global information to identify relevant sources	Opportunity to develop systematic review skills and thematic coding techniques.	Adopt structured search strategies; use citation management tools to organise and filter sources efficiently.

	required significant time and effort.		
Conflicting Perspectives	The literature presented various and sometimes contradictory viewpoints on cybersecurity strategies and governance.	Enabled critical thinking and the synthesis of a balanced conceptual framework.	Apply comparative analysis to reconcile differences; prioritise peer-reviewed and high-impact sources for reliability.
Time Constraints	Balancing the literature review with other research activities under strict timelines posed a challenge.	Encouraged the adoption of efficient review strategies and time management techniques.	Use project management tools; set clear milestones for the completion of the literature review completion; allocate dedicated time blocks for focused reading.

7.3 Challenges and opportunities encountered during data generation

According to Rimando et al. (2015, p. 2025), data collection is critical to the social research process and, when done correctly, it improves the quality of the study. Every researcher is bound to encounter difficulties in collecting data. Like any other researcher, the researcher has faced some significant challenges that were not anticipated at the outset. These challenges and opportunities are presented in Table 7-2.

Table 7-2: Summary of recommendations in alignment to the objectives.

Challenges	Description of Challenge	Opportunities	Recommendations
Availability of participants	Difficulty in recruiting managers, IT professionals, and employees due to after-work commitments, such as family responsibilities and transportation schedules.	With the help of the Municipal Manager, participants were recruited after work hours, ensuring adequate representation and insight into the phenomenon.	Plan interviews considering participant schedules; engage management early to facilitate availability; include flexible options such as virtual interviews where possible.
Lack of willingness to participate in the research	Participants were reluctant to participate in verbal interviews, preferring written responses due to discomfort or fear of confidentiality breaches.	Explaining confidentiality and ethical compliance encouraged participation, leading to signed consent forms and improved trust.	Conduct pre-interview sessions to explain the purpose, benefits, and confidentiality; provide written assurances and consent forms to build trust.
Time management during interviews	Technical glitches and irrelevant questions caused delays, risking data quality and exceeding agreed time slots.	Negotiating extensions helped recover lost time without compromising research objectives.	Allocate buffer time in interview schedules; prepare contingency plans for technical issues; prioritise essential questions to maintain data quality.
Working with familiar colleagues	Familiarity led to a lack of seriousness among some colleagues, affecting cooperation and timely data collection.	The management intervention improved cooperation and facilitated access to the necessary data.	Maintain professional boundaries; involve senior management for oversight; communicate research objectives clearly to colleagues to ensure seriousness.

Misunderstandings during interviews	Questions and clarifications sometimes disrupted flow, creating confusion, and slowing progress.	Real-time clarification improved data integrity and participant confidence.	Provide a comprehensive briefing before interviews; encourage participants to ask questions; clarify any confusion promptly during sessions.
Ethical Considerations	Participants hesitated to participate and commit to a study due to ethical reasons	Formal ethical clearance was secured prior to data collection, guaranteeing adherence to university policies on academic integrity and responsible research conduct.	Provide participants with complete disclosure of study objectives, risks, and rights; obtain written informed consent; anonymise data to protect privacy; ensure no harm or discomfort; maintain honesty and integrity in data collection and reporting.

7.4 Conclusion

Conducting research in a sensitive area like cybersecurity within the public sector is never straightforward. The challenges faced during the literature review and data collection were not just obstacles, they became opportunities to improve the research process. Issues such as conflicting points of view, participant availability, and ethical concerns required flexible and creative solutions. These experiences reinforced the importance of planning, ethical responsibility, and adaptability in producing credible results. Ultimately, the lessons learnt here will help future researchers navigate similar challenges and strengthen the quality and integrity of their work.

CHAPTER 8

Conclusions and future studies

8.1 Introduction

This chapter brings this study to a close by reviewing the research objectives and explaining how they were achieved. The main aim was to improve cybersecurity awareness strategies within the South African local government by making informed recommendations based on the existing literature and practical insights from gamified training. This was achieved through an extensive review of relevant studies, the identification of best practices, and the integration of gamification principles into awareness strategies.

Secondary objectives were also successfully met. On the theoretical side, this study explored existing frameworks and gamification techniques, identified appropriate tools, and consolidated recommendations from the literature. Empirically, surveys, focus groups, and semi-structured interviews provided valuable information on employees' awareness levels and their experiences with gamified training tools. Together, these efforts informed a comprehensive set of recommendations aimed at strengthening cybersecurity awareness in local government settings of South Africa.

8.2 Conclusion

Combining gamification techniques with traditional cybersecurity awareness methods offered meaningful insights into improving employee engagement and knowledge retention. Previous research confirmed that gamification can enhance learning and drive behavioural change (Deterding et al., 2011; Hsu & Chiu, 2014). This study found that many local government employees misunderstand cybersecurity risks and best practices, a finding consistent with previous studies linking poor awareness with increased vulnerability (Hadnagy, 2018). Introducing targeted gamified training helped address these misconceptions and created a stronger culture of security literacy. The case study approach added depth to the analysis by capturing employee experiences and attitudes toward cybersecurity. Based on these findings, this study recommended that policy-makers adopt gamified strategies in cybersecurity training programmes to improve effectiveness and participation.

8.3 Recommendations for future research

Future research should explore the long-term impact of gamified cybersecurity training through longitudinal studies, focussing on behavioural change and threat reduction over time. Comparative studies between gamified and traditional training methods in different local government contexts would provide further insight into effectiveness. There is also a need to design and develop serious games tailored to South African or broader African settings, incorporating culturally relevant elements. Furthermore, research should investigate which game mechanics, such as points, levels, storytelling, and rewards, work best in public sector environments. These efforts will help create sustainable, engaging and impactful cybersecurity awareness programmes.

References

- Abbadia, J. (2022). Research Paradigm: An introduction with examples. Mind the Graph. <https://mindthegraph.com/blog/research-paradigm>.
- Abduhari, E.S., Shaik, T.C., Adidul, A.B., Ladjia, J.H., Saliddin, E.S., Adin, A.J., Rumbahali, F.A., Sali, A.B., Jemser, J.M. and Tahil, S.K. (2025) ‘Access Control Mechanisms and Their Role in Preventing Unauthorized Data Access: A Comparative Analysis of RBAC, MFA, and Strong Passwords’, Natural Sciences Engineering and Technology Journal, 5(1), pp. 418–430.
- Abdullah, M., Nawaz, M.M., Saleem, B. (2025). Evolution Cybercrime—Key Trends, Cybersecurity Threats, and Mitigation Strategies from Historical Data. Analytics, 4(3), 25; <https://doi.org/10.3390/analytics4030025>
- Abedeji, K.B., Abu-Mahfouz, A.M. and Kurien, A.M. (2023) ‘DDoS Attack and Detection Methods in Internet-Enabled Networks: Concept, Research Perspectives, and Challenges’, Journal of Sensor and Actuator Networks, 12(4), p. 51. <https://doi.org/10.3390/jsan12040051>
- Ackerman, B., Nguyen, T.Q. and Stuart, E. (2019) *Sensitivity Analysis for Unobserved Effect Modification when Generalizing Findings from Randomized Trials to Target Populations*. Johns Hopkins Bloomberg School of Public Health. Available at: <https://washstat.org/presentations/20190610/20190610_Ackerman.pdf> (Accessed: 27 July 2025).
- Adams, T. and Painter, M. (2019) Managing Risk in Information Systems. Burlington, MA: Jones & Bartlett Learning. Available at: <https://www.jblearning.com/catalog/productdetails/9781284183719> (Accessed: 1 August 2025).
- Adedeji, K.B., Abu-Mahfouz, A.M. & Kurien, A.M., 2023. DDoS attack and detection methods in internet-enabled networks: Concept, research perspectives, and challenges. Journal of Sensor and Actuator Networks, 12(4), p.51. Available at: <https://doi.org/10.3390/jsan1204005>

- Admass, W.S., Munaye, Y.Y., and Diro, A.A. (2024). Cyber security: State of the art, challenges and future directions, *Cyber Security and Applications*, 2, <https://doi.org/10.1016/j.csa.2023.100031>.
- AICPA (American Institute of Certified Public Accountants), 2020. Service Organisation Control (SOC). [online] Available at: <https://www.aicpa.org> [Accessed 1 Aug. 2025].
- AICPA, 2023. SOC 2 Trust Services Criteria. [online] Available at: <https://www.aicpa-cima.com/topic/audit-assurance/audit-and-assurance-greater-than-soc-2> [Accessed 5 Oct. 2025].
- Ajzen, I. (1991) ‘The theory of planned behavior’, *Organizational Behavior and Human Decision Processes*, 50(2), pp. 179–211. [https://doi.org/10.1016/0749-5978\(91\)90020-T](https://doi.org/10.1016/0749-5978(91)90020-T)
- Alenezi, M., Nadeem, M. and Asif, R. (2021) ‘SQL injection attacks countermeasures assessments’, *Indonesian Journal of Electrical Engineering and Computer Science*, 21(2), pp. 1121–1131.
- Alhussein, M., Alafifah, A. and Alhothali, M. (2020) ‘The Effect of Gamification on Learning Outcomes in Cybersecurity Education’, *International Journal of Information and Education Technology*, 10(3), pp. 227–231.
- Ali Ahmed, Watterson, C., Alhashmi, S. and Gaber, T. (2024) ‘How universities teach cybersecurity courses online: a systematic literature review’, *Frontiers in Computer Science*, 6. <https://doi.org/10.3389/fcomp.2024.1499490>
- Alkhalil, Z., Hewage, C., Nawaf, L. and Khan, I. (2021) ‘Phishing attacks: A recent comprehensive study and a new anatomy’, *Frontiers in Computer Science*, 3, p. 563060.
- Almeida, M., de Carvalho, N. and Guerreiro, T. (2017) ‘Digital crime and security: The importance of cybersecurity awareness in organisations’, *Journal of Computer Virology and Hacking Techniques*, 13(2), pp. 65–72.
- Al-Mohammed, B.A. & Baydoun, A., 2024. You Are the First Line of Defense: Integrating Humans into Information Security Frameworks. In: 2024 International Conference on Computer and Applications (ICCA), pp.1–11. IEEE.

- Alotaibi, R., 2020. Gamification in cybersecurity awareness: A systematic review. *Journal of Cybersecurity and Privacy*, 1(2), pp.225–240. Available at: <https://doi.org/10.3390/jcp1020015>
- Aman, W. and Al Shukaili, J., 2021. A classification of essential factors for the development and implementation of cyber security strategy in public sector organizations. *International Journal of Advanced Computer Science and Applications*, 12(8).
- Amin, R.M., Cloppert, M.J. & Hutchins, E.M., 2011. Intelligence-driven cyber defence benefits from an understanding of adversarial campaigns and intrusion kill chains. Lockheed Martin Corporation. Available at: <https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf> [Accessed 1 Aug. 2025].
- Arroyabe, M.F., Arranz, C.F.A., De Arroyabe, I.F., De Arroyabe, J.C.F. (2024). Revealing the realities of cybercrime in small and medium enterprises: Understanding fear and taxonomic perspectives. *Computers & Security*, 141, p.103826 <https://doi.org/10.1016/j.cose.2024.103826>
- Australian Cyber Security Centre, 2021. Essential Eight. Available at: <https://www.cyber.gov.au>.
- Bada, A., Sasse, M.A. & Nurse, J.R.C., 2019. Cyber Security Awareness Training: Understanding the Effectiveness of the Best Practices. *Cyber Security: A Peer-Reviewed Journal*, 2(3), pp.1–17.
- Bairagi, V. and Munot, M.V. (2019) *Research Methodology: A Practical and Scientific Approach*. Boca Raton: CRC Press. DOI: <https://doi.org/10.1201/9781351013277> (Accessed: 03 September 2025).
- Baker, C., 2019. Focus groups in research: Qualitative data collection and analysis. *Journal of Social Research*, 45(2), pp.100–115.
- Bălăceanu, C. & Iliescu, M., 2018. Gamification in cybersecurity training: engaging employees in defensive behaviours. *Computers & Security*, 78, pp.471–485.

- BankservAfrica (2024) Payments News Round-Up. Available at: <https://www.bankservafrika.com/blog/post/6d10bb1a-bca9-4888-a6e6-3c6852a6d45b_payments-news-round-up> (Accessed: 27 April 2025).
- Begum, H., Khan, S. & Ramzan, M., 2018. Ethical considerations in research. *International Journal of Research*, 5(1), pp.1–6.
- Bell, D.E. & LaPadula, L.J., 1973. *Secure Computer Systems: Mathematical Foundations*. MITRE Corporation.
- Benaroya, K., 2018. *Cybersecurity Management: A guide for the Healthcare Industry*. Healthcare Information and Management Systems Society.
- Bendovschi, A., 2015. Trends, patterns, and security countermeasures. *Procedia Economics and Finance*, 28, pp.24–31. [https://doi.org/10.1016/S2212-5671\(15\)01077-1](https://doi.org/10.1016/S2212-5671(15)01077-1)
- Bhana, S., Goundan, S. & Aucamp, G., 2022. Adoption of Cybersecurity Awareness Programs: A Review of Key Challenges and Opportunities. *Information Technology & People*, 35(5), pp.1233–1252.
- Bhandari, P., 2023. What is quantitative research? Definition, uses & methods. Scribbr. Available at: <https://www.scribbr.com/methodology/quantitative-research/> [Accessed 12 Aug. 2024].
- Biba, K.J., 1977. *Integrity Considerations for Secure Computer Systems*. Bedford, MA: MITRE Corporation. Available at: <https://apps.dtic.mil/sti/citations/ADA039324> [Accessed 5 Oct. 2025].
- Bilge, L. & Dumitraş, T., 2012. Before we knew it: an empirical study of zero-day attacks in the real world. In: *Proceedings of the 2012 ACM conference on Computer and communications security*, pp.833–844.
- Binns, R., Harrington, B. & Williams, T., 2021. The Importance of Cybersecurity for Local Governments. *Journal of Public Administration*, 45(3), pp.45–62.
- Booth, A., Sutton, A. & Papaioannou, D., 2016. *Systematic Approaches to a Successful Literature Review*. London: Sage Publications.
- Bostrom, R.P. & Heinen, J.S., 1977. MIS problems and failures: A sociotechnical perspective. *MIS Quarterly*, 1(3), pp.17–32.

- Botha (2021) *Cybersecurity readiness in South African Public Sector Organisations*. University of Johannesburg. Available at: <<https://ujcontent.uj.ac.za/esploro/outputs/graduate/Cybersecurity-readiness-in-South-African-Public/9927106007691>> (Accessed: 27 April 2025).
- Boyson, S., 2014. Cyber Supply Chain Risk Management: Revolutionizing the Strategic Control of Critical IT Systems. *Technovation*, 34(7), pp.342–353.
- Braun, V. & Clarke, V., 2024. Thematic analysis. In: *Encyclopedia of quality of life and well-being research*, pp.7187–7193. Cham: Springer International Publishing.
- Calder, A., 2023. *Cyber Essentials: A Guide to the Cyber Essentials and Cyber Essentials Plus Certifications*.
- CAV, 2020. *Cybersecurity Framework*. National Institute of Standards and Technology. Available at: <https://www.nist.gov/cyberframework>
- Chandra, A., 2020. Measurement of the Cloud Security Level at Company using Cloud Control Matrix.
- Chatchalernpun, S. and Daengsi, T. (2021) ‘Improving cybersecurity awareness using phishing attack simulation’, *IOP Conference Series: Materials Science and Engineering*, 1088(1), 012015. DOI: <https://doi.org/10.1088/1757-899X/1088/1/012015> (Accessed: 27 October 2024).
- Chetty, P., 2013. Importance of a case study in research. Project Guru. Available at: <https://www.projectguru.in/importance-of-a-case-study-in-research/> [Accessed 1 Aug. 2025].
- Choo, K.-K.R., 2016. The cyber threat landscape: Challenges and future directions. *Journal of Strategic Security*, 9(4), pp.99–125.
- CIS (Center for Internet Security), 2021. *CIS Critical Security Controls*. Available at: <https://www.cisecurity.org>.
- CIS. (2024). *CIS Controls v8*. Center for Internet Security.
- City of Cape Town. (2021). *CyberSmart Program Evaluation*. Cape Town: Local Government.
- Cloud Security Alliance (CSA). (2021). *Cloud Controls Matrix (CCM)*. Available at: <https://cloudsecurityalliance.org>.

- Conti, M., Dragoni, N. and Lesyk, V. (2016). A survey of man-in-the-middle attacks. *IEEE Communications Surveys & Tutorials*, 18(3), pp.2027–2051. <https://doi.org/10.1109/COMST.2016.2548426>
- Creemers, R. (2022). Cybersecurity threats and challenges in local government: A South African perspective. *South African Journal of Information Management*, 24(1), pp.1–9.
- Creswell, J.W. and Creswell, J.D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches*. 5th ed. Thousand Oaks, CA: Sage.
- Creswell, J.W. and Poth, C.N. (2018). *Qualitative inquiry and research design: Choosing among five approaches*. 4th ed. Thousand Oaks, CA: Sage.
- CSIR. (2024). National survey results on the state of cybersecurity in South Africa. Council for Scientific and Industrial Research. Available at: <https://www.csir.co.za/national-survey-results-on-state-cybersecurity-south-africa>
- D’Arcy, J., Herath, T. and Shoss, M. (2021) ‘Understanding employee responses to stressful information security requirements: A coping perspective’, *Journal of Management Information Systems*, 31(2), pp. 285–318. DOI: <https://doi.org/10.1080/07421222.2021.1870389> (Accessed: 22 November 2024).
- Da Vinci Forensics. (2025). CIPC breached. Available at: <https://davinciforensics.co.za/cybersecurity/cipc-breached/>
- Dahl, J. and Eckstein, S. (2018). Implementing the NIST cybersecurity framework: A practical approach. In *NIST Cybersecurity Framework*, pp.1–24. NIST.
- Davis, F.D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), pp.319–340. <https://doi.org/10.2307/249008>
- Davis, F.D. and Tullis, T. (2010). A usefulness or usability? In *Proceedings of the 2010 ACM Conference on Computer Supported Cooperative Work*, pp.205–208.
- Davis, F.D., Venkatesh, V., Morris, M.G. and Davis, G.B. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 27(3), pp.425–478. <https://doi.org/10.2307/30036540>

- Davis, L., Matlosa, K. and Mthethwa, Z. (2023). Navigating cyber threats in local governance: A South African perspective. *International Journal of Cyber Policy*, 5(1), pp.22–40.
- de Villiers, M.R., de Villiers, P.J.T. & Kent, A.P. (2005) ‘The Delphi technique in health sciences education research’, *Medical Teacher*, 27(7), pp.639–643. doi: 10.1080/13611260500069947.
- Department of Communications and Digital Technologies (DCDT). (2021). Annual Report 2020/21. Available at: https://www.gov.za/sites/default/files/gcis_document/202110/communicationsdigitaltechnologies202021.pdf [Accessed 16 June 2025].
- Department of Communications and Digital Technologies (DCDT). (2020) Strategic Plan 2020–2025. [pdf] Pretoria: Government of South Africa. Available at: <https://www.dcdt.gov.za/documents/strategic-plans/file/54-strategic-plan-2020-2025.html>
- Department of Communications and Digital Technologies. (2016). National Cybersecurity Policy Framework. South African Government.
- Department of Cooperative Governance. (2021). Cybersecurity strategy for South African local government. Pretoria: Republic of South Africa. Available at: <https://www.cogta.gov.za/index.php/docs/state-of-local-government-report-2021/> [Accessed 23 June 2025].
- Department of State Security. (2015). National Cybersecurity Policy Framework (NCPF). Government Gazette, No. 39475, 4 December. Available at: https://www.gov.za/sites/default/files/gcis_document/201512/39475gon609.pdf [Accessed 03 July 2025].
- Deterding, S. (2012). Gamification: Designing for motivation. In *Proceedings of the 2012 annual conference on human factors in computing systems*, pp.201–206. ACM. <https://doi.org/10.1145/2212877.2212883>
- Deterding, S., Khaled, R., Nacke, L.E. and Dixon, D. (2011). Gamefulness: Defining “gamification”. In *Proceedings of the 15th International Academic MindTrek Conference: Envisioning Future Media Environments*, pp.9–15. ACM. <https://doi.org/10.1145/2181037.2181040>

- Dlodlo, N. (2020). Cybersecurity challenges in local government: Empirical insights from South Africa. *Journal of Information Security and Applications*, 50, pp.76–86.
- DOE. (2014) Cybersecurity Capability Maturity Model (C2M2). U.S. Department of Energy.
- Donaldson, L. (2001) *The Contingency Theory of Organizations*. Thousand Oaks, CA: Sage Publications. Available at: <https://us.sagepub.com/en-us/nam/the-contingency-theory-of-organizations/book10668> [Accessed 1 Aug. 2025].
- Donekal, A., Singh, R., and Patel, M., 2024. Enhancing Cybersecurity Awareness through Gamified XR and AI Simulations. *Journal of Cybersecurity Education and Practice*, 9(2), pp.112–130.
- Donekal, S., Ramesh, A. and Pillai, V. (2024) ‘Enhancing Cybersecurity Awareness through Gamified Extended Reality Training’, *International Journal of Cyber Education*, 9(2), pp. 101–118. Available at: <https://doi.org/10.3390/info15120814>.
- Donekal, S., Zhong, Y. and Liu, H. (2024) ‘Enhancing Cybersecurity Awareness through Gamified Extended Reality Training’, *International Journal of Cyber Education*, 8(2), pp. 101–118.
- Dutta, T.S. (2025) ‘Microsoft SharePoint Server 0-Day Hack Hits African Treasury, Companies, and University’, *Cybersecurity News*. Available at: <https://cybersecuritynews.com/microsoft-sharepoint-server-0-day-hack/>.
- Elhami, A. (2022) ‘Conducting an interview in qualitative research’, *Mextesol Journal*, 46(1).
- Empirical Studies on Gamification. (2014) 47th Hawaii International Conference on System Sciences, pp. 3025–3034. IEEE.
- ENISA. (2020) *Cybersecurity Framework*. European Union Agency for Cybersecurity. Available at: <https://www.enisa.europa.eu/>.
- eScribe Meetings (2025) ‘Challenges in Municipal Cybersecurity Training’, *Municipal Technology Journal*, 18(2), pp. 34–47.
- eThekwini Local Government. (2021) *Cybersecurity Quest: Program Overview*. Durban: Local Government.

- Faghani, A. and Salehi, M. (2020) 'Human Factor in Cybersecurity: A Literature Review', *Journal of Information Security*, 11(2), pp. 75–82. Available at: <https://link.springer.com/article/10.1007/s10207-025-01032-0>.
- Fischer, M. (2020) 'Assessing the Effectiveness of Cybersecurity Awareness Training', *Computers & Security*, 95, 101971. Available at: <https://doi.org/10.1093/cybsec/tyac006>.
- Ford, J.K. (2014) 'Assess training effectiveness: A review of best practices', *Theory into Practice*, 53(2), pp. 189–197.
- Gcaza, N. and Von Solms, R., 2017. A strategy for a cybersecurity culture: A South African perspective. *The Electronic Journal of Information Systems in Developing Countries*, 80(1), pp.1-17.
- GCR. (2020) *Global Cybersecurity Frameworks: A Comparison*.
- Gee, J.P. (2003) 'What Video Games Have to Teach Us About Learning and Literacy', *Computers in Human Behavior*, 19(1), pp. 199–202.
- Gee, J.P. (2005) *Games without Frontiers: Stories in Political Philosophy*. TELIC Press.
- Gee, J.P. (2008) 'Learning and games', in Shaffer, K.S., Squire, D. and Halverson, R. (eds.) *Games and Simulations in Online Learning: Research and Development Frameworks*. Hershey, PA: IGI Global, pp. 40–46.
- George, J. (2024) 'Cyber resilience in South Africa: from regulatory mandate to strategic imperative', *Compli-Serve*. Available at: <https://compliserve.co.za/2145-2/> [Accessed 11 Aug. 2025].
- Gill, P., Stewart, K., Treasure, E. and Chadwick, B. (2008) 'Methods of data collection in qualitative research: interviews and focus groups', *British Dental Journal*, 204(6), pp. 291–295.
- Given, S. (2024) *A Review of South Africa's National Cybersecurity Policy Framework: Progress and Challenges After Nearly a Decade*. Institute for Digital Security and Innovation. Available at: <https://idsi.org.za> [Accessed 23 Sep. 2025].
- Glover, I. (2013) 'Play and learn: A framework for gamification in education', in *The Impact of Gaming on Education and Training*. Melbourne: Routledge.

- Gordon, L.A., Loeb, M.P. and Zhou, L. (2020) 'Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model', *Journal of Cybersecurity*, 6(1). Available at: <https://doi.org/10.1093/cybsec/tyaa005>.
- Government of South Africa. (2020) Cyber Crimes Act. Available at: <https://www.gov.za/documents/acts/cybercrimes-act-19-2020-english-afrikaans-01-jun-2021> [Accessed 1 Aug. 2025].
- Government Technology. (2025) 'Cybersecurity Vulnerabilities in Local Government'. [online] Available at: <https://www.govtech.com> [Accessed 10 May 2025].
- Granger, M.D., et al. (2018) 'An exploratory study of mode efficacy in cybersecurity training', *Journal of Cybersecurity Education, Research and Practice*, 2021(1), Article 2. Available at: <https://files.eric.ed.gov/fulltext/EJ1338314.pdf> (Accessed: 23 November 2024).
- Gross, S., Fregni, F. and Brunoni, A. (2018) *Study Population*. In: *Critical Thinking in Clinical Research: Applied Theory and Practice Using Case Studies*. Oxford University Press. Available at: <https://academic.oup.com/book/24450/chapter/187497446> (Accessed: 27 May 2025).
- Hadnagy, C. (2010) *Social Engineering: The Science of Human Hacking*. Hoboken, NJ: John Wiley & Sons.
- Hadnagy, C. (2018) *Social Engineering: The Science of Human Hacking*. Hoboken, NJ: Wiley.
- Hämäläinen, M., 2024. Analysis of artificial intelligence in cybersecurity identity and access management: potential for disruptive innovation.
- Hamari, J., Koivisto, J. & Sarsa, H., 2014. Does gamification work?--A literature review of empirical studies on gamification. In: *Proceedings of the 47th Hawaii International Conference on System Sciences*. IEEE, pp.3025–3034.
- Hardie, L. (2025) 'South Africa's government and military organisations face 3,480 attacks per week', *Intelligent CIO Africa*, 2 June. Available at: <https://www.intelligentcio.com/africa/2025/06/02/south-africas-government-and-military-organisations-face-3480-attacks-per-week/> (Accessed: 27 November 2025).

- Hasani, T., O'Reilly, N., Dehghantanha, A., Rezania, D. and Levallet, N., 2023. Evaluating the adoption of cybersecurity and its influence on organizational performance. *SN Business & Economics*, 3(5), p.97.
- Henrico, S., & Els, S. (2025). Cyber Attacks in South Africa: Geopolitical and legal implications. *African Security Review*, 34(3), 312–336. <https://doi.org/10.1080/10246029.2025.2489352>
- Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, 18(2), 106–125.
- Herrmann, D. & Pridöhl, H., 2020. Basic Concepts and Models of Cybersecurity. In: M. Christen et al., eds. *The Ethics of Cybersecurity. The International Library of Ethics, Law and Technology*, vol. 21. Springer. Available at: https://doi.org/10.1007/978-3-030-29053-5_2
- Higgins, L., Joseph, P., & McDonnell, S. (2019). Evaluating the NIST Cybersecurity Framework through qualitative analysis: A case study of a local government. *International Journal of Information Privacy, Security and Integrity*, 4(2), 115-130.
- HITRUST Alliance. (2021). HITRUST Common Security Framework. Retrieved from <https://hitrustalliance.net>
- HITRUST. (2024). HITRUST CSF Overview. HITRUST Alliance.
- Hollis, S., Wilkins, D. T., & Reinemann, K. (2018). Cybersecurity Awareness: Strategies for Improving Engagement with Employees. *Journal of Business Continuity & Emergency Planning*, 12(2), 108-114.
- Hoseini, S. and Majidi Gahrodi, N., 2023. Investigating The Effect of Social Engineering Techniques on Employees Vulnerability (Case study: Tehran Municipality Employees). *Electronic and Cyber Defense*, 11(1), pp.31-46.
- Howlett, M. (2022) 'Looking at the "field" through a Zoom lens: Methodological reflections on conducting online research during a global pandemic', *Qualitative Research*, 22(3), pp. 387–402. DOI: <<https://doi.org/10.1177/1468794120985691>> (Accessed: 23 November 2024)

- Hsu, C.-L. and Chiu, C.-M. (2014) ‘A Longitudinal Study of User Acceptance of Gamification in Online Learning’, *Journal of Educational Technology & Society*, 17(4), pp. 103–113.
https://researchspace.csir.co.za/bitstream/handle/10204/13563/Abu-Mahfouz7_2023.pdf
- Huitema, R. and Wong, T., 2025. Gamified Cryptography: A Case Study in Cybersecurity Training. *Cybersecurity Pedagogy Review*, 7(1), pp.55–70.
- Hussain, J. (2022). Virtual Private Networks: Fundamentals, Security Issues and Solutions. SSRN. Available at SSRN: <https://ssrn.com/abstract=4478285> or <http://dx.doi.org/10.2139/ssrn.4478285>
- Hussein and Ndlovu (2021) The evolving Cyber Security threat in Africa. Liquid Intelligent Technologies Report. Available at: <https://liquid.tech/wp-content/uploads/2023/01/LiquidIntelligentTechnologiesCybersecurityReport2021.pdf> (Accessed: 20 March 2025).
- IBM (2021) *Cost of a Data Breach Hits Record High During Pandemic*. Available at: <https://newsroom.ibm.com/2021-07-28-IBM-Report-Cost-of-a-Data-Breach-Hits-Record-High-During-Pandemic> (Accessed: 27 February 2025).
- Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, 31(1), 83–95.
- INTERPOL (2021) African Cyberthreat Assessment Report. Available at: <https://www.interpol.int> [Accessed: 16 September 2025].
- INTERPOL. (2024). African Cyberthreat Assessment Report 2024. Available at: https://www.interpol.int/en/content/download/21048/file/24COM005030-AJFOC_Africa%20Cyberthreat%20Assessment%20Report_2024_complet.pdf
- ISACA. (2018). COBIT Framework. ISACA. Retrieved from <https://www.isaca.org/resources/cobit>
- ISACA. (2021). Cybersecurity Awareness: Building a Culture of Security. ISACA. Retrieved from <https://www.isaca.org/resources/isaca-journal/issues/2021/volume-4/cybersecurity-awareness-building-a-culture-of-security>
- ISACA. (2023). COBIT 2019 Framework. ISACA.

- ISO (2018) ISO/IEC 27005:2018 Information technology – Security techniques – Information security risk management. Geneva: International Organization for Standardization.
- ISO (International Organization for Standardization). (2021). ISO 27000 Series. Retrieved from <https://www.iso.org>
- ISO, 2013. ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements. Geneva: International Organization for Standardization.
- ISO. (2012). ISO/IEC 27032:2012 - Guidelines for cyber security. International Organization for Standardization.
- ISO. (2022). ISO/IEC 27001: Information Security Management. International Organization for Standardization.
- ISO/IEC 27001. (2013). Information technology — Security techniques — Information security management systems — Requirements. International Organization for Standardization.
- IT-Online, 2025. Strategic partnerships play a role in municipal cybersecurity. [online] Available at: <<https://it-online.co.za/2025/03/14/strategic-partnerships-play-a-role-in-municipal-cybersecurity/>> [Accessed 31 July. 2025].
- James, A. (2016). Evaluating the effectiveness of employee training programs: A data-driven approach. *International Journal of Information Systems for Crisis Response and Management*, 8(2), 55-68.
- Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, 34(3), 549–566.
- Jones, D. & Ashenden, D. (2021). Quantifying Cyber Risk with FAIR. *Journal of Cyber Risk Analysis*, 9(2), 45-60.
- Kang, M., Ryu, S.-O., & Choi, Y. (2020). The Role of Feedback in Gamification: The Moderating Effect of Enjoyment. *Computers in Human Behavior*, 104, 106-114.
- Kaplan, J. (2017). Understanding behavioral metrics in cybersecurity. *Information Security Journal: A Global Perspective*, 26(3), 123-132.

- Kapp, K. M. (2012). *Gamification on Learning and Instruction: Game-based Methods and Strategies for Training and Education*. John Wiley & Sons.
- Kaspersky. (2020). *Cybersecurity in local government: Understanding the challenges*. Retrieved from <<https://www.kaspersky.com>>
- Kaspersky. (2024). *What is Credential Stuffing?* Available at: <<https://www.kaspersky.co.za/blog/what-is-credential-stuffing/33220/>>
- Kathayat, A.S. (2024) ‘Advanced SQL Injection: Exploitation Techniques & Prevention Strategies’, DEV Community. Available at: <https://dev.to/abhay_yt_52a8e72b213be229/advanced-sql-injection-exploitation-techniques-prevention-strategies-2fab> (Accessed: 13 July 2025).
- Kennedy, D., O’Gorman, J., Kearns, D. and Aharoni, M., 2011. *Metasploit: The Penetration Tester’s Guide*. San Francisco, CA: No Starch Press. ISBN: 978-1-59327-288-3.
- Khanna, P., 2023. Emerging cybersecurity threats and countermeasures: A comprehensive review. *International Journal of Creative Research Thoughts*, [online] 11(7), pp.1–15. Available at: <<https://ijcrt.org/papers/IJCRT2307659.pdf>> [Accessed 11 Aug. 2025].
- Kharas, D. (2019). *City of Johannesburg ransomware attack highlights cybersecurity vulnerabilities*. BusinessTech. Retrieved from <<https://businesstech.co.za/news/government/349519/city-of-johannesburg-ransomware-attack-highlights-cybersecurity-vulnerabilities/>>
- Kim, D., & Gilman, K. (2016). Understanding the impact of gamification on learning outcomes: A review of the literature. *Journal of Educational Technology Systems*, 44(4), 420-433.
- Kim, J., Zhong, L. and Liu, Y., 2025. Enhancing Cybersecurity Education through Gamified Learning. *Journal of Information Security Education*, 18(2), pp.112–130.
- Kivunja, C. & Kuyini, A. B. (2017). Understanding and applying research paradigms in educational contexts. *International Journal of higher education*, 6(5), 26-41.
- Klein, H. K., & Myers, M. D. (1999). A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems. *Management Information Systems Quarterly*, 23(1), 67-93.

- Kok, D. (2020). The challenges of cybersecurity compliance in public sector organizations. *South African Journal of Information Management*, 22(1), 1-9.
- Korstjens, I. & Moser, A., 2018. Series: Practical guidance to qualitative research. Part 4: Trustworthiness and publishing. *European Journal of General Practice*, 24(1), pp.120–124.
- Kumar, S., & Singhal, A. (2020). Analysis of South African Cyber Act and its significant impact on the cyber law scenario. *International Journal of Cyber Criminology*, 14(1), 300-307.
- Landers, R. N. (2014). Developing a theory of gamified learning: Linking serious games and gamification of learning. In *Learning, Education and Games: Volume Two: 100 Games for the Classroom* (pp. 91-115).
- Landers, R. N., Bauer, K. N., & Callan, R. C. (2017). Development of a gamified learning objective system: A view from psychology and education. *Journal of Education and Human Development*, 6(2), 1-12.
- Letseka, G.T. (2022). Cybersecurity readiness in South African Public Sector Organisations. MCom Thesis, University of Johannesburg. Available at: <<https://hdl.handle.net/10210/504155>>
- Levine, E.E. & Schweitzer, M.E., 2014. Are liars ethical? On the tension between benevolence and honesty. *Journal of Experimental Social Psychology*, 53, pp.107–117.
- Li, J., Feng, B., Zheng, H. (2025). A survey on VPN: Taxonomy, roles, trends and future directions, *Computer Networks*, 257, <https://doi.org/10.1016/j.comnet.2024.110964>.
- Liamputtong, P. (2009). Qualitative data analysis: conceptual and practical considerations. *Health promotion journal of Australia*, 20(2), 133-139.
- Liñan-Acosta, B., Bazalar-Gonzales, O. and Santisteban, J., 2025, August. Frameworks for Cyberattack Prevention: A Comparative Analysis. In *2025 International Conference on Artificial Intelligence, Computer, Data Sciences and Applications (ACDSA)* (pp. 1-5). IEEE.
- Lincoln, Y.S. & Guba, E.G., 1985. *Naturalistic inquiry*. Beverly Hills, CA: Sage.
- Mabaso, N.J. (2018). Assessing the cyber-security status of the metropolitan local governments in South Africa. PhD Thesis, University of KwaZulu-Natal. Available at:

<<https://researchspace.ukzn.ac.za/bitstreams/f5b73415-0c71-4d1a-bb9c-d852b66df0ee/download>>

- Mabunda, S. (2021). Cybersecurity in South Africa: Towards Best Practices. In: DeNardis, L., Musiani, F., & Cogburn, D.L. (eds.) *CyberBRICS*. Springer, pp. 227–270. Available at: <https://link.springer.com/chapter/10.1007/978-3-030-56405-6_6>
- Madhlangobe, L., Chinomona, R., & Moyo, T. (2022). The role of gamified training in improving cybersecurity awareness in South African governments. *Journal of Information Security Research*, 14(2), 45-63.
- Malele, V. and Mphasane, K. (2025) “Safeguarding Mobile Users from Violation by Third-party Apps”, *Latin-American Journal of Computing*, 12(1), pp. 27–34. doi: 10.5281/zenodo.14448505.<https://doi.org/10.5281/zenodo.14448505>.
- Manpreet, K. B. (2017) data analysis and its importance: *International research journal of advanced engineering and science*, Guru Gobind Singh indraprastha university.
- Marakalala, M.C. and Madzivhandila, A.C., 2025. An Overview of Forensic Investigators in the Investigation of Mobile Fraud: The Study Case of the South African Banking Industry. *OIDA International Journal of Sustainable Development*, 18(09), pp.99-110.
- Marciano, T., du Toit, J. and Maluleka, S., 2024. Gamification and Attitude Shifts in Cybersecurity Training. *South African Journal of Information Security*, 15(1), pp.55–70.
- Martin, B. and Shapiro, M. (2020). 'A Contingency Theory Approach to Adaptive Cybersecurity Strategies', *Journal of Cybersecurity*, 5(2), pp. 134–150. Available at: <https://academic.oup.com/cybersecurity> [Accessed 1 Aug. 2025].<https://academic.oup.com/cybersecurity>
- Martínez, J. and Durán, J.M., 2021. Software supply chain attacks, a threat to global cybersecurity: SolarWinds’ case study. *International Journal of Safety and Security Engineering*, 11(5), pp.537-545.
- Mathew, A., 2023. The 5 cs of cybersecurity and its integration with predictive analytics. *International Journal of Computer Science and Mobile Computing*, 12(1), pp.47-50.
- Matovu, R., Nwokeji, J.C., Holmes, T. & Rahman, T., 2022. Teaching and learning cybersecurity awareness with gamification in smaller universities and colleges. 2022 IEEE

- Frontiers in Education Conference (FIE), Uppsala, Sweden, pp.1–9. Available at: <https://doi.org/10.1109/FIE56618.2022.9962519>. Republic of South Africa, 1996. The Constitution of the Republic of South Africa Act 108 of 1996. Pretoria: Government Printer.
- Meriah, I. and Rabai, L.B.A., 2019. Comparative study of ontologies based iso 27000 series security standards. *Procedia Computer Science*, 160, pp.85-92.
- Mertler, C.A. (2021). Action Research as Teacher Inquiry: A Viable Strategy for Resolving Problems of Practice. *Practical Assessment, Research, and Evaluation*, 26(19).
- Microsoft (2024) Digital Defense Report. Available at: <https://www.microsoft.com> (Accessed: 16 September 2025).<https://www.microsoft.com>
- Mitnick, K.D. and Simon, W.L., 2002. *The Art of Deception: Controlling the Human Element of Security*. New York, NY: Wiley Publishing.
- MITRE (2024) MITRE ATT&CK Framework. Available at: <https://attack.mitre.org> (Accessed: 16 September 2025).<https://attack.mitre.org>
- MITRE. (2021). MITRE ATT&CK™ Framework. Retrieved from <https://attack.mitre.org/https://attack.mitre.org/>
- MITRE. (2023). MITRE ATT&CK Framework. MITRE Corporation.
- Moher, D., Liberati, A., Tetzlaff, J., Altman, D.G. & PRISMA Group (2009) ‘Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement’, *PLoS Medicine*, 6(7), e1000097. doi: 10.1371/journal.pmed.1000097.
- Mokheti, M., Moshoeshoe, A., & Mphahlele, R. (2021). Enhancing cybersecurity training in local government through gamification. *International Journal of Cybersecurity and Digital Forensics*, 10(3), 1-15.
- MoldStud Research, 2024. Enhancing Cybersecurity Awareness Through Gamified Learning. *International Journal of Cyber Education*, 9(1), pp.33–47.
- Monyamane, M., & Mphahlele, M. (2020). The influence of municipal socio-economic characteristics on innovation adoption in South African local government. *African Journal of Science, Technology, Innovation and Development*, 12(4), 477-487

- Moore, A., Cole, E. and Ring, E. (2020). 'A Realistic Approach to Addressing the Cyberthreat Environment', *Journal of Cybersecurity Research*, 15(1), pp. 37–50. Available at: <https://academic.oup.com/cybersecurity> [Accessed 1 Aug. 2025].<https://academic.oup.com/cybersecurity>
- Mpuru, L. & Kgoale, C. (2025). Recognizing the evolving cybercrime threats in South Africa. *African Security*. Available at: <https://doi.org/10.1080/19392206.2025.2515302><https://doi.org/10.1080/19392206.2025.2515302>
- Munn, Z., Peters, M.D.J., Stern, C. et al. Systematic review or scoping review? Guidance for authors when choosing between a systematic or scoping review approach. *BMC Med Res Methodol* 18, 143 (2018). <https://doi.org/10.1186/s12874-018-0611-x><https://doi.org/10.1186/s12874-018-0611-x>
- Muntean, C. I. (2011). Raising engagement in e-learning through gamification. In *Proceedings of the 6th international conference on virtual learning environments* (pp. 323-329).
- Munyani, M., Tsoeu, M., & Mamashela, S. (2020). Assessing Cybersecurity Awareness in Local Government in South Africa. *African Journal of Public Affairs*, 10(2), 40-56.
- Mzileni, B., & Nyoni, T. (2022). Skills Shortage in Cybersecurity: An Analysis of Local Governments in South Africa. *African Journal of Information Systems*, 14(2).
- Narkhede, S. (2020) Sources of Data Collection: Primary and Secondary. *GeeksforGeeks*. Available at: <https://www.geeksforgeeks.org/macro-economics/sources-of-data-collection-primary-and-secondary-sources/> (Accessed: 27 January 2025)
- National Cybersecurity Advisory Council. (2021). South Africa Cybersecurity Strategy. Retrieved from https://www.gov.za/sites/default/files/gcis_document/201512/39475gon609.pdfhttps://www.gov.za/sites/default/files/gcis_document/201512/39475gon609.pdf
- National Institute of Standards and Technology (NIST). (2014). Framework for Improving Critical Infrastructure Cybersecurity. Gaithersburg, MD: U.S. Department of Commerce. Available at: <https://csrc.nist.gov/pubs/itlb/2014/02/framework-for-improving-critical-infrastructure-cy/final> [Accessed 1 Aug.

2025].<https://csrc.nist.gov/pubs/itlb/2014/02/framework-for-improving-critical-infrastructure-cy/final>

NEC XON. (2025). Credential Theft Surges in South Africa. Available at: <https://www.nec.africa/news/credential-theft-surges-in-south-africa-nec-xon-issues-critical-cybersecurity-warning><https://www.nec.africa/news/credential-theft-surges-in-south-africa-nec-xon-issues-critical-cybersecurity-warning>

Negrão de Andrade, T. et al. (2025). Zero-Day Vulnerabilities and the Clandestine Exploits Market: A Hermeneutic and Critical Approach. *IOSR Journal of Humanities and Social Science*, 30(1), pp.11–20. Available at: <https://www.iosrjournals.org/iosr-jhss/papers/Vol.30-Issue1/Ser-7/B3001071120.pdf><https://www.iosrjournals.org/iosr-jhss/papers/Vol.30-Issue1/Ser-7/B3001071120.pdf>

networks. CSIR ResearchSpace. Available at:

Ngejane, H. (2024) Data Breaches in South Africa: Survey Report. Pretoria: CSIR. Available at:

<https://www.csir.co.za/sites/default/files/Documents/241013_CSIR%20Infographic%20posters_Draft%204_Data%20breaches.pdf> (Accessed: 15 May 2025).

Ngulube, P. (2022). *Handbook of Research on Mixed Methods Research in Information Science*. IGI Global.

NIST (2011) SP 800-30 Rev. 1: Guide for Conducting Risk Assessments. Gaithersburg: National Institute of Standards and Technology.

NIST (2012) Guide for Conducting Risk Assessments. SP 800-30 Rev. 1. Gaithersburg: National Institute of Standards and Technology.

NIST (2018). Framework for improving critical infrastructure cybersecurity. Retrieved from <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.03462018.pdf>

NIST (2024). Cybersecurity Framework 2.0. National Institute of Standards and Technology.

Nkosi, V., & Sutherland, W. (2023). Gamified simulations as a means to improve decision-making skills in cybersecurity scenarios for local government employees. *South African Journal of Information Management*, 25(1), 8-21.

- Nkwanyana, S. (2020). Nelson Mandela Bay Local government cyberattack: What we know so far. ITWeb. Retrieved from <<https://itweb.co.za/news/3g06pYe8Wb9gNnM5>>
- Norris, D., Mateczun, L., Joshi, A., and Finin, T. (2021). Managing cybersecurity at the grassroots: Evidence from the first nationwide survey of local government cybersecurity. *Journal of Urban Affairs*, 43(8), 2021, pp. 1173-1195, <https://doi.org/10.1080/07352166.2020.1727295>
- Ntuli, T. and Puthan, P. (2020) *National Cybersecurity Implementation in South Africa: The Conundrum Question*. *Journal of Information Warfare*, 21(1), pp. 1–16. Available at: <<https://www.jstor.org/stable/27199954>> (Accessed: 27 April 2025).
- Nwokeji, Joshua C.; Matovu, Richard; and Rawal, Bharat, "THE USE OF GAMIFICATION TO TEACH CYBERSECURITY AWARENESS IN INFORMATION SYSTEMS" (2020). Proceedings of the 2020 AIS SIGED International Conference on Information Systems Education and Research. 29. <https://aisel.aisnet.org/siged2020/29>
- O'Connor, S. (2019). The art of feedback in cybersecurity training. *Cybersecurity Awareness Review*, 23(1), 5-10.
- Odlum, M., & Yates, C. (2021). Cybersecurity Vulnerabilities in South African Local governments: Recommendations for Capacity Building. *Journal of Governmental Affairs*, 8(3), 302-316.
- Oriokot, L., Buwembo, W., Munabi, I.G. et al., 2011. The introduction, methods, results and discussion (IMRAD) structure: a survey of its use in different authoring partnerships in a students' journal. *BMC Research Notes*, 4(250). <https://doi.org/10.1186/1756-0500-4-250>.
- Osanaiye, O., Choo, K.K.R. and Dlodlo, M., 2016. Distributed denial of service (DDoS) resilience in cloud: Review and conceptual cloud DDoS mitigation framework. *Journal of Network and Computer Applications*, 67, pp.147-165.
- Overberg District Municipality. (2022). Municipal Corporate Governance of Information and Communication Technology Policy. Available at: <https://odm.org.za> [Accessed 23 Sep. 2025].
- OWASP (2023) OWASP Top 10 Web Application Security Risks. Available at: <https://owasp.org> (Accessed: 16 September 2025).

- Pappas, I. O., & Koutsouris, D. (2018). Gamification and Cybersecurity: A Review. *International Journal of Information Management*, 39, 174-182.
- Parliament of the Republic of South Africa. (2002). Electronic Communications and Transactions Act. Retrieved from https://www.gov.za/sites/default/files/gcis_document/201409/a25-02.pdf
- PCI Security Standards Council. (2018). PCI DSS Standards. Retrieved from <https://www.pcisecuritystandards.org/>
- PCI Security Standards Council. (2020). PCI-DSS Standards. Retrieved from <https://www.pcisecuritystandards.org>
- Peltier, T. R. (2016). *Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management*. Boca Raton: Auerbach Publications. <https://doi.org/10.1201/9780849390326>
- Peltier, T.R. (2006). *Information Security Fundamentals*. Boca Raton, FL: Auerbach Publications. Available at: <https://www.routledge.com/Information-Security-fundamentals/Peltier/p/book/9781439810620> [Accessed 1 Aug. 2025].
- Peyper, L. (2024). SA's Government Departments Are Sitting Ducks for Cyber Attacks. Moneyweb. Available at: <https://www.moneyweb.co.za/qa/sas-government-departments-are-sitting-ducks-for-cyber-attacks/>
- Pfleeger, S.L., Sasse, M.A. and Furnham, A. (2014) 'Human behaviour and security: Why do users make poor decisions?', *IEEE Security & Privacy*, 12(4), pp. 62–68. DOI: <https://doi.org/10.1109/MSP.2014.68> (Accessed: 27 August 2024).
- Pieterse, H. (2021). The cyber threat landscape in South Africa: A 10-year review. *The African Journal of Information and Communication*, 28, pp. 1–21. Available at: <https://doi.org/10.23962/10539/32213>
- Pillay and Naidoo (2021) *Aligning South African Data and Cloud Policy with the PoPI Act*. Stellenbosch University. Available at: <https://pdfs.semanticscholar.org/9c78/1eaf8d81c17ccabe1aa5f8be3102c24f1e86.pdf> (Accessed: 20 March 2025).

- Prasad, R. and Rohokale, V., 2019. Cyber threats and attack overview. In *Cyber Security: The Lifeline of Information and Communication Technology* (pp. 15-31). Cham: Springer International Publishing.
- Presidency of South Africa, 2019. National Intelligence Estimate 2019–2024. [online] Available at: <https://www.thepresidency.gov.za/media-statement-minister-presidency-khumbudzo-ntshavheni-release-national-security-strategy-2024> [Accessed 11 Aug. 2025].
- Prümmer, J., Van Steen, T., Van den Berg, B. (2024). A systematic review of current cybersecurity training methods *Computers & Security*, Vol. 136. <https://doi.org/10.1016/j.cose.2023.103585>
- PwC (2023) *Cyber and Digital Technology Risks Are a Key Concern for Businesses and Risk Leaders*. Available at: <https://www.pwc.com/gx/en/news-room/press-releases/2023/cyber-and-digital-technology-risks-are-a-key-concern-for-businesses-and-risk-leaders.html> (Accessed: 07 June 2025).
- Qollakaj, K., Larsson, L.E., and Memeti, S. (2025). Cybersecurity of remote work migration: A study on the VPN security landscape post Covid-19 outbreak. *Array* (27). <https://doi.org/10.1016/j.array.2025.100437>
- Republic of South Africa, 2002. Electronic Communications and Transactions Act 25 of 2002. Government Gazette, [online] Available at: <https://www.gov.za/documents/electronic-communications-and-transactions-act> [Accessed 16 Aug. 2025].
- Republic of South Africa, 2013. Protection of Personal Information Act 4 of 2013. Government Gazette, No. 37067, 26 November. [online] Available at: https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013popi.pdf [Accessed 11 June. 2025].
- Republic of South Africa, 2020. Cybercrimes Act 19 of 2020. Government Gazette, [online] Available at: <https://www.gov.za/documents/acts/cybercrimes-act-19-2020-english-afrikaans-01-jun-2021> [Accessed 11 May. 2025]
- Republic of South Africa, 2021. Cybercrimes Act No. 19 of 2020. Government Gazette, [online] Available at: <https://www.gov.za/documents/acts/cybercrimes-act-19-2020-english-afrikaans-01-jun-2021> [Accessed 01 Aug. 2025].

- Republic of South Africa. (2000). Municipal Systems Act 32 of 2000. Government Printer.
- Republic of South Africa. (2020). Cyber Crimes Act 19 of 2020. Government Printer.
- Resnik, D.B., 2015. What is ethics in research & why is it important? National Institute of Environmental Health Sciences.
- Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology*, 91(1), 93–114.
- Rogers, R.W., 1983. Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In: J.T. Cacioppo & R.E. Petty, eds. *Social Psychophysiology: A Sourcebook*. New York: Guilford Press, pp.153–176.
- Rogers, Y., Sharp, H., & Preece, J. (2020). *Interaction Design: Beyond Human-Computer Interaction*. John Wiley & Sons.
- Roopesh, M., 2024. Cybersecurity solutions and practices: Firewalls, IDS/IPS, encryption, MFA. *Academic Journal on Business Administration, Innovation & Sustainability*, 4(3), pp.37–52. Available at: <https://core.ac.uk/download/pdf/624121394.pdf>
- SABRIC (2024) Annual Crime Statistics Report. Available at: <https://www.sabric.co.za>
- Safa, N. S., et al. (2016). Information security policy compliance: A theory of planned behavior perspective. *Computers & Security*, 56, 70–82.
- Sailer, M., Hense, J. U., Mayr, S. K., & Mandl, H. (2017). How gamification motivates: An experimental study of the effects of gamification on student learning. *Computers & Education*, 105, 1-12.
- SALGA. (2012). *ICT Governance Guidelines for Municipalities*. South African Local Government Association. Available at: <https://salga.org.za>
- SALGA. (2022). *Cybersecurity Awareness in Local Government: The Current State and Future Directions*. South African Local Government Association.
- Sani, A., Olajide, A., Ogunsanya, V., Oyeboode, D., Alfred, J., Oseni, T., Jegede, E., Nwaogu, N. and Abbas, R., 2025. Cybersecurity Challenges in Digitizing Government Administration. *Proceedings of the International Academy of Sciences*, 2(1), pp.1-13.

- SANS Institute. (2020). Security Operations Center (SOC). Retrieved from <https://www.sans.org>
- SANS. (2021). The Critical Security Controls. SANS Institute. Retrieved from <https://www.sans.org/critical-security-controls/>
- Sasse, M.A. (2020) *Free and Low-Cost Online Cybersecurity Learning Content*. NIST. Available at: <https://www.nist.gov/itl/applied-cybersecurity/nice/resources/online-learning-content> (Accessed: 20 July 2025).
- Saunders, M., Lewis, P. & Thornhill, A., 2019. Research methods for business students. 8th ed. Harlow: Pearson Education.
- Schoenfeld, J., 2024. Cyber risk and voluntary Service Organization Control (SOC) audits. *Review of Accounting Studies*, 29(1), pp.580-620.
- SECNORA, 2025. Cybersecurity Training Through Gamification: Real-World Impact. *Journal of Cyber Behavior*, 18(2), pp.112–128.
- Sharif, F., 2024. Enhancing Cyber Security Resilience: Phishing Defense and the Importance of Measurement Strategies.
- Shead, A. D., Rouse, J., & Babich, M. (2020). Applying gamification to online cybersecurity training: a case study. *International Journal of Information Security*, 19(2), 203-214.
- Shingange, G., 2024. A review of South Africa's National Cybersecurity Policy Framework: Progress and challenges after nearly a decade. Available at: <https://idsi.org.za/2024/07/26/a-review-of-south-africas-national-cybersecurity-policy-framework-progress-and-challenges-after-nearly-a-decade/>
- Shostack, A., 2014. Threat Modeling: Designing for Security. Hoboken, NJ: John Wiley & Sons.
- Sithaldeen, R. (2024). Using action research and grounded theory techniques to design an evidence-based academic advising programme. *Journal of Student Affairs in Africa*, 12(2), 37–50. DOI: 10.24085/jsaa.v12i2.5452

- Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*. Volume 104, November 2019, Pages 333-339. <https://doi.org/10.1016/j.jbusres.2019.07.039>
- Sollaci, L.B. and Pereira, M.G., 2004. The introduction, methods, results, and discussion (IMRAD) structure: a fifty-year survey. *Journal of the Medical Library Association*, 92(3), pp.364–367. Available at: <<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC442179/>> [Accessed 20 October 2025].
- Sommestad, T., 2012. A framework and theory for cyber security assessments (Doctoral dissertation, KTH Royal Institute of Technology).
- Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, 36(2), 215–225.
- South African Government, 2020. Cybersecurity Awareness Month Campaign. Available at: <https://www.education.gov.za/ArchivedDocuments/ArchivedArticles/Cybersecurity-Awareness-Month-1023.aspx>
- South African Government. (2013). Protection of Personal Information Act. Retrieved from https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013popi.pdf
- State Security Agency. (2015). National Cybersecurity Policy Framework for South Africa. *Government Gazette No. 39475*. Available at: https://www.gov.za/sites/default/files/gcis_document/201512/39475gon609.pdf
- Stewart, K., 2025. Understanding South African cybersecurity law in the context of the recent SAA cyber incident. Available at: <https://www.polity.org.za/article/understanding-south-african-cybersecurity-law-in-the-context-of-the-recent-saa-cyber-incident-2025-07-31>
- Steyn, M., Bothma, J., & Nkosi, M. (2020). Barriers to Cybersecurity in Local Government: An Empirical Study. *Journal of Administrative Sciences*, 43(2), 31-44.
- Sullivan, K., Sheahan, J., & O'Brien, K. (2019). Diversity and Inclusion in Cybersecurity: Engaging New Audiences through Gamification. *International Journal of Information Management*, 47, 1-9.

- Sutherland, E. (2017). Governance of Cybersecurity – The Case of South Africa. *The African Journal of Information and Communication*, 20. Available at: <https://scielo.org.za>
- TechCentral (2024) The true cost of a data breach in South Africa. Available at: <https://techcentral.co.za/true-cost-of-a-data-breach-south-africa/248934/> (Accessed: 02 November 2025).
- Thagaard, T. (2018) *Systematic Approaches to Qualitative Research*. Bergen: Fagbokforlaget. Summary available at: <https://www.simplypsychology.org/qualitative-research-characteristics-design-methods-examples.html> (Accessed: 13 January 2025).
- Tracy, S.J. (2024) *Qualitative Research Methods: Collecting Evidence, Crafting Analysis, Communicating Impact*. 3rd edn. Hoboken: Wiley-Blackwell. Available at: <https://www.wiley.com/en-us/Qualitative+Research+Methods%3A+Collecting+Evidence%2C+Crafting+Analysis%2C+Communicating+Impact%2C+3rd+Edition-p-9781119988670> (Accessed: 22 January 2025)
- Tshabalala, T., and Shukla, S. (2021). An Examination of Cybersecurity Challenges through the Lens of Contingency Theory. Pages 220–234 of *The Information Security Journal*, Volume 12, Issue 4.
- Tsohou, A., Rapture, E., & Lee, P. (2019). The Importance of Cybersecurity Awareness: A Computer-Supported Collaboration Perspective. *Internet of Things*, 5, 66-79.
- Turin, T. C., Chowdhury, N. & Raihan, M. (2024). Decoding research: Philosophical pillars of research paradigms. *Bangabandhu Sheikh Mujib Medical University Journal*, 17(2), e73249-e73249.
- UK National Cyber Security Centre. (2021). *Cyber Essentials*. Retrieved from <https://www.ncsc.gov.uk>.
- Utz, J. (2023). What is a research paradigm? Types of research paradigms with examples.
- Urhuogo, O. and Addo, R., 2024. Bridging the Cybersecurity Skills Gap: A Gamification Model. *Journal of Cybersecurity Education, Research and Practice*, 12(1), pp.45–62.

- Urhuogo, O. and Addo, R., 2024. Bridging the Cybersecurity Skills Gap: A Gamification Model. *Journal of Cybersecurity Education, Research and Practice*, 12(1), pp.45–62.
- Van der Merwe, C., Zulu, J., & Ndlovu, T. (2023). User engagement and participation in gamified cybersecurity training: A South African perspective. *African Journal of Cybersecurity*, 4(2), 23-36.
- van der Merwe, E., 2023. Comparative Legal Perspectives on Business Email Compromise: An In-Depth Study of South African and United States Law with a Focus on Fiduciary Obligations and Cybersecurity Measures. University of Johannesburg (South Africa).
- Van Grembergen, W., & De Haes, S. (2018). *Enterprise Governance of IT: A Analysis Tool for IT Managers*. Springer.
- Van Heerden, R., Von Soms, S. and Mooi, R., 2016, May. Classification of cyber attacks in South Africa. In *2016 IST-Africa Week Conference* (pp. 1-16). IEEE.
- Van Niekerk, J., & Von Solms, R. (2015). A holistic framework for the fostering of an information security sub-culture in organizations. *Information Management & Computer Security*, 23(4), 381-431.
- Vance, A., Phillips, A., & Haines, C. (2021). Cybersecurity Awareness Programs: What Works? *Computers & Security*, 107, 102198.
- Venkatesh, V. and Davis, F.D., 2000. A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Science*, 46(2), pp.186–204.
- Verizon (2024) Data Breach Investigations Report. Available at: <https://www.verizon.com> [Accessed: 16 September 2025].
- Wabiser, Y.D. and Singgalen, Y.A., 2022. An Evaluation of Control Objective for Information Related Technology (COBIT) 4.0 or 4.1: Systematic Literature Review. *Journal of Information Systems and Informatics*, 4(2), pp.300-320.
- Wang, H., & Sui, M. (2016). Gamification: A New Approach to Information Security Awareness Training. *Journal of Information Technology Education: Innovations in Practice*, 15, 61-76.
- Wang, L., Ma, Z., & Zhang, H. (2016). A Study of Cybersecurity Awareness Training Effectiveness Using Pre- and Post-Test Assessment. *Computers & Security*, 60, 140-149.

- White, G.B. and Sjelin, N., 2022. The NIST cybersecurity framework. In Research anthology on business aspects of cybersecurity (pp. 39-55). IGI Global.
- Whitman, M.E. and Mattord, H.J. 2018. Principles of Information Security. 7th ed. Boston, MA: Cengage Learning. Available at: <https://www.cengage.com/c/principles-of-information-security-7e-whitman/mattord/9780357506431/?searchIsbn=9780357506431> [Accessed 1 Aug. 2025].
- Whitney, K. (2019). Evaluating the Long-Term Effectiveness of Cybersecurity Training. *Journal of Cybersecurity Education, Research and Practice*, 2(1), 1-12.
- Whitton, N. (2014). *Learning with Digital Games: A Practical Guide to Engaging Students in Higher Education*. Routledge.
- Wognum, N., et al. (2021) *Interactive Training Modules – ThreatReady Resources*. Available at:
<<https://www.getthreatready.com/cybersecurity-training/interactive-training-modules/>>
(Accessed: 17 November 2024).
- Yulianto, S., Lim, C. and Soewito, B., 2016, May. Information security maturity model: A best practice driven approach to PCI DSS compliance. In 2016 IEEE Region 10 Symposium (TENSYP) (pp. 65-70). IEEE.
- Zhang, C., Wang, J., & Liu, Y. (2022). Enhancing Local Government Cybersecurity through Public-Private Partnerships. *Governance & Cybersecurity Journal*, 8(3), 95-113.
- TechCentral (2023) The human attack vector: Social engineering. Available at:
<<https://techcentral.co.za/the-human-attack-vector-social-engineering-avaprom/205781/>>
(Accessed: 02 November 2025).

Annexure A: Ethics approval letter of study



Private Bag X1290, Potchefstroom
South Africa 2520
Tel: 018 299-1111/2222
Fax: 018 299-4910
Web: <http://www.nwu.ac.za>
Senate Committee for Research Ethics
Tel: 0169103446
Email: Feziwe.Mseleni@nwu.ac.za

ETHICS APPROVAL LETTER OF STUDY

Based on approval by the Faculty of Natural and Agricultural Sciences Ethics Committee (FNASREC), the Faculty of Natural and Agricultural Sciences Ethics Committee hereby approves your study as indicated below. This implies that the North-West University Senate Committee for Research Ethics (NWU-SCRE) grants its permission that, provided the special conditions specified below are met and pending any other authorisation that may be necessary, the study may be initiated, using the ethics number below.

Study title: Recommendation for cyber-security awareness for the South African local government using a gamification approach
Study Leader/Supervisor: Prof Vusumuzi Malele
Student: Mr Giyani Hlungwani

Ethics number:

NWU-01495-24-A9

Status: S – Submission; R – Re-Submission; P – Provisional Authorisation; A – Authorisation

Application Type: Single study
Commencement date: 18-02-2025

Risk Category:

Minimal

Expiry date: 18-05-2026
Approval of the study is initially provided for a year, after which continuation of the study is dependent on receipt and review of the annual (or as otherwise stipulated) monitoring report and the concomitant issuing of a letter of continuation.

Special in process conditions of the research for approval (if applicable):

- The following documentation are archived by FNASREC and should be complete and kept up to date:
 - Research proposal
 - Signed approval from the scientific committee indicating the proposed risk category
 - All researchers involved in the study should submit signed NWU code of conduct statements annually.
 - All researchers of low-risk studies should submit proof of relevant ethics training every three years.
 - All researchers that take part in activities that pose a safety and security threat to the researchers, or the environment should submit a risk assessment form annually.
 - All research involving human interaction should follow best ethical practice and keep documents as proof. This includes informed consent, questionnaires, incorporation of risk-benefit, and responsible data management.
 - Any research at governmental or private institutions, permission must still be obtained from relevant authorities and provided to the FNASREC. Ethics approval is required BEFORE approval can be obtained from these authorities.

1

Special conditions:

The best practices with regards to interviews should be implemented, including proper negotiation of access to participants; representative sampling; documented informed consent that includes the important elements; alignment of information collected with research questions; anonymization of collected information, ensuring the integrity and security of all data collected.

General conditions:

While this ethics approval is subject to all declarations, undertakings and agreements incorporated and signed in the application form, the following general terms and conditions will apply:

- The study leader/supervisor (principal investigator)/researcher must report in the prescribed format to the FNASREC:
 - annually (or as otherwise requested) on the monitoring of the study, whereby a letter of continuation will be provided, and upon completion of the study; and
 - without any delay in case of any adverse event or incident (or any matter that interrupts sound ethical principles) during the course of the study.
- The approval applies strictly to the proposal as stipulated in the application form. Should any amendments to the proposal be deemed necessary during the course of the study, the study leader/researcher must apply for approval of these amendments at the FNASREC, prior to implementation. Should there be any deviations from the study proposal without the necessary approval of such amendments, the ethics approval is immediately and automatically forfeited.
- Annually a number of studies may be randomly selected for an external audit.
- The date of approval indicates the first date that the study may be started.
- In the interest of ethical responsibility, the NWU-SCRE and FNASREC reserves the right to:
 - request access to any information or data at any time during the course or after completion of the study;
 - to ask further questions, seek additional information, require further modification or monitor the conduct of your research or the informed consent process.
 - withdraw or postpone approval if:
 - ◇ any unethical principles or practices of the study are revealed or suspected.
 - ◇ it becomes apparent that any relevant information was withheld from the FNASREC or that information has been false or misrepresented.
 - ◇ submission of the annual (or otherwise stipulated) monitoring report, the required amendments, or reporting of adverse events or incidents was not done in a timely manner and accurately; and / or
 - ◇ new institutional rules, national legislation or international conventions deem it.
- FNAS-REC can be contacted for further information or any report templates via Nomali.Ngobese@nwu.ac.za

The FNASREC would like to remain at your service as scientist and researcher, and wishes you well with your study. Please do not hesitate to contact the FNASREC or the NWU-SCRE for any further enquiries or requests for assistance.

Yours sincerely

Prof Nomali Ngobese
Chairperson Faculty of Natural and Agricultural Sciences Ethics Committee (FNAS-REC)

Signature: Nomali Ngobese
nomali.ngobese@nwu.ac.za
Email: nomali.ngobese@nwu.ac.za

Annexure B: Letter of permission to conduct research

225 Collins Chabane Dr
Old DCO Building
Malamulele
0982



Private Bag X9271
Malamulele
0982
Tel (015) 851 0110
Fax (015) 851 0097

COLLINS CHABANE LOCAL MUNICIPALITY

Ref: 4/4/R
ENQ: MAPUTLA TMD
CELL: 072 766 0852

26/03/2024

Mr Hlungwani G.P
P.O Box .
Malamulele
0982

Dear Sir/ Madam

**SUBJECT: LETTER OF PERMISSION TO CONDUCT RESEARCH FOR MR
HLUNGWANI GIYANI PHANUEL.**

1. The above matter refers.
2. This serves to confirm that **Mr Hlungwani Giyani Phanuel of ID No 760317 5350 085** has been granted a permission to conduct research in Collins Chabane Local Municipality.
3. The research is based on "Cybersecurity Awareness Strategy through Gamification".
4. Hope you find this in order.

Regards


**SHILENGE R.R.
MUNICIPAL MANAGER**

Vision: "A spatially integrated and sustainable local economy by 2030"

Mission: To ensure the provision of sustainable basic services and infrastructure to improve the quality of life of our people and to grow the local economy for benefit of all citizens

Annexure C: Invitation to participate



Invitation to participate in a master's research project on cybersecurity awareness.

Dear Collen Radali

I hope this message finds you well. My name is Hlungwani Giyani and I am a graduate student at Northwest University pursuing my Master's degree in Computer Science. I am conducting a research project that aims to recommend cybersecurity awareness in South African local governments using a gamification approach.

As part of this study, I invite you to participate in a collaborative process that includes engaging in a brief game designed to raise awareness about cybersecurity challenges, followed by a questionnaire and a follow-up interview. Your perspectives and experiences would greatly enrich this research and help to develop effective recommendations.

Here is what participation entails:

1. Engagement with a game: you will play a gamified application focused on cybersecurity for approximately 15 minutes.
2. Questionnaire: after the game, you will complete a questionnaire that will take about 15 minutes.
3. Follow-up Interview: finally, a follow-up interview lasting approximately 30 minutes will be conducted to discuss your thoughts and feedback in more detail.

The total time commitment for your participation will be around 1 hour. Please be assured that all information collected will remain confidential and will be used solely for the purpose of this investigation.

If you are interested in participating or would like to know more, feel free to reach out to me at giyanih@gmail.com or 0834009476. I would be happy to provide further details and answer any questions you may have.

Thank you for considering this invitation. Your contribution is vital to the success of this project and I truly appreciate your time and commitment.

Best regards,

A handwritten signature in blue ink, appearing to be 'H. Giyani', is placed above the contact information.

Hlungwani Giyani
Northwest University
giyanih@gmail.com
083 400 9476

Annexure D: Consent to participate



CONSENT FORM

Purpose:

The purpose of this research study is to recommend the cyber-security awareness for the South African local government using a gamification approach. By participating in this study, you will contribute to the advancement of knowledge in the field of cybersecurity awareness and potentially help improve the cybersecurity practices within the South African local government.

Study Procedures:

If you agree to participate, you will be asked to:

1. Complete an initial questionnaire to assess your current level of cybersecurity knowledge and awareness.
2. Engage in a gamified initiative specifically designed to impart cybersecurity knowledge through interactive games and challenges.
3. Participate in a follow-up questionnaire and provide feedback on the gamified training endeavour to determine the efficacy of the gamified cybersecurity strategy in raising your cybersecurity awareness.

Risks and Benefits:

While the risk associated with this study is minimal, there is a possibility of minor frustration or fatigue due to the participation requirements or technological difficulties. However, the potential benefits of participating include enhancing your cybersecurity knowledge, contributing to the enhancement of effective cybersecurity strategy, and potentially improving cybersecurity practices within the South African local government.

Confidentiality and Data Handling:

Your participation in this study will be completely anonymous and confidential. All data collected will be securely stored and only accessed by the research team. Any information collected

during this study will only be used for research purposes and will be reported in aggregate form, ensuring that no individual can be identified.

Voluntary Participation and Withdrawal:

Participation in this study is entirely voluntary, and you have the right to withdraw at any time without penalty or explanation. Your decision to participate or withdraw will not affect your relationship with Collins Chabane Local Municipality.

Contact Information:

If you have any questions, concerns, or require further information about this study, please contact me or my supervisor. Our details are provided below:

Supervisor Name: Professor. Vusi Malele
Phone Number: 082 077 5398
Email Address: Vusi.Malele@nwu.ac.za

Researcher Name: Giyani Hlungwani
Phone Number: 083 400 9476
Email Address: giyanih@gmail.com

By signing this consent form, you acknowledge that you have read and understood the study's purpose, procedures, risks, benefits, confidentiality, and your right to withdrawal.

By signing below, you confirm your voluntary participation in the research study:

Signature of participant:

Date:

Signature of researcher:

Date:

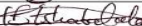

03 March 2025

03/03/2025

Annexure E: Focus group attendance register

FOCUS GROUP ATTENDANCE REGISTER FOR EMPLOYEES
12-Mar-25

Master's research project on cybersecurity awareness

Code E	Names	Designation	Contact Number	Email Address	Signature
1	Beauty Hlungwani				
2	Caswell Linda	Accountant	0730438709	Caswell.Linda@collinslabans.co.za	
3	Clarah Shabangu				
4	Cyril Mafuleke	Secretary Gen committee officer	07947385438	Cymafuleke@gmail.com	
5	Dokodola Hasane	Reserve Lic	0723772785	Funnyhasane@yahoo.com	
6	Giyani Hlungwani		0664225968	giyani1@gmail.co	
7	Hlamfani Tshabatala	Secretary: BTO	0727676540	Hthamfani-BTO@gmail.com	
8	Hlulani Mabunda				
9	Lucan Marilele	Secretary	0670231195	lucanmarilele@gmail.com	
10	Mahlori Chauke	Payroll clerk	0724368712	maahlori.chauke@gmail.com	
11	Mbhonci Manganyini	valuation officer	0784004036	mumanganyini@hotmail.co.za	
12	Millicent Mojela				
13	Nkululeko Mabaso	Town Planner	0728250802	nkululeko.mabaso@collinslabans.co.za	

14	Oupa Mabasa				
15	Pamela Mafuleke				
16	Phathu Masuvhelele				
17	Prodah Manganyi				
18	Respect Mashole				
19	Rirhandzu Chabalala	RECORDS CLERK	067 132 1122	Rirhandzu Chabalala r.chabalala@ccm.gov.za	
20	Sydney Khubayi				
21	Tintwalo Ntshalati	Records Clerk	025160734	Tintwalo Ntshalati tntwalo@ccm.gov.za	
22	Tinyiko Makhubele	LAND USE OFFICER	0660251508	Tinyiko Makhubele t.makhubele@ccm.gov.za	
23	Tsakani Siweya				
24	Vusi Makhasa				
25	Ntshuxeko Maswanganye				
26	Nfanelo Mabunda				
27	Masali Ndumeni	Registry Clerk	0728235551	Charlotte Ndumeni c.ndumeni@ccm.gov.za	

28. Mathonsi
Livingstone

Building
Contact office 0660852962

Charlotte ndymen
Collinscharlene goetz ~~Consent~~

Livingstone mathias
Collinscharlene goetz ~~Consent~~

Annexure F: Cybersecurity awareness questionnaire



QUESTIONNAIRE

Code: *EP*

Research Study Topic: Recommendations for cyber-security awareness for the South African local government using a gamification approach.

Introduction

Thank you for participating in this study; your insights are vital. Please answer the questions honestly and feel free to elaborate on your thoughts. All responses will be kept confidential.

Section 1: Demographic Information

1. What is your age range?

- ☐ 18-24

- ☒ 25-34

- ☐ 35-44

- ☐ 45-54

- ☐ 55+

2. What is your gender

- ☐ Female

- ☒ Male

- ☐ Prefer not to say

3. What is your occupation within the municipality?

- ☒ Employee
- ☐ IT Professional
- ☐ Management
- ☐ Other (please specify): _____

4. What is your role within the municipality?

- ☐ Management
- ☐ IT Section
- ☒ Administrative Staff
- ☐ Other (Please specify): _____

5. How long have you been working in this role?

- ☐ Less than 1 year
- ☐ 1-3 years
- ☐ 4-6 years
- ☒ More than 6 years

6. What is your level of education?

- ☐ Diploma
- ☒ Bachelor's Degree
- ☐ Master's Degree
- ☐ Other (Please specify): _____

Section 2: Knowledge Assessment Questions

7. On a scale of 1 to 5, how would you rate your knowledge of cybersecurity before playing the trivia twirl game?

- ☐ 1 - Very low
- ☐ 2 - Low
- ☒ 3 - Average
- ☐ 4 - High
- ☐ 5 - Very high

8. On a scale of 1 to 5, how would you rate your knowledge of cybersecurity after playing the trivia twirl game?

- ☐ 1 - Very low
- ☐ 2 - Low
- ☐ 3 - Average
- ☒ 4 - High
- ☐ 5 - Very high

9. How confident do you feel about your cybersecurity knowledge after playing the game?

- ☐ Not confident at all
- ☐ Slightly confident
- ☐ Moderately confident
- ☒ Very confident
- ☐ Extremely confident

10. Did you learn any new concepts or facts about cybersecurity while playing the game?

- ☒ Yes
- ☐ No

- If yes, please provide examples: The risk of using Hotel WiFi and setting of password

11. Which specific topics do you feel you improved your knowledge on?

(Select all that apply)

- ☒ Phishing
- ☒ Password security
- ☐ Malware
- ☐ Data protection
- ☒ Safe internet practices
- ☐ Other: _____

12. How likely are you to apply what you learned from the game in real-life situations?

- ☐ Not likely
- ☐ Slightly likely
- ☐ Moderately likely
- ☐ Very likely
- ☒ Extremely likely

Section 3: Emotional Response Questions

13. How did you feel about your learning experience during the trivia twirl game?

(Select all that apply)

- ☒ Engaged
- ☒ Motivated
- ☐ Overwhelmed
- ☒ Inspired
- ☐ Confused
- ☐ Other:

14. Did the game change your perception of cybersecurity?

- ☒ Yes
- ☐ No

- If yes, please explain: We need protect our information through Cyber security

15. How would you describe your overall satisfaction with the trivia twirl game in terms of learning?

- ☐ Very dissatisfied
- ☐ Dissatisfied
- ☐ Neutral
- ☒ Satisfied
- ☐ Very satisfied

16. On a scale of 1 to 5, how much do you feel your knowledge has improved as a result of playing the game?

- ☐ 1 - Not at all
- ☐ 2 - A little
- ☐ 3 - Somewhat
- ☐ 4 - Quite a bit
- ☒ 5 - A great deal

17. Which areas of cybersecurity do you feel you learned the most about? (Select all that apply)

- ☒ Phishing
 - ☐ Password security
 - ☐ Malware
 - ☒ Data protection
 - ☒ Safe browsing practices
 - ☐ Other:
-

18. Did you encounter any questions that challenged your existing knowledge?

- ☐ Yes
 - ☒ No
 - If yes, please provide examples:
-

19. How confident do you feel applying what you learned in real-life situations?

- ☐ Not confident at all
- ☐ Slightly confident
- ☐ Moderately confident
- ☒ Very confident
- ☐ Extremely confident

20. How did playing the trivia twirl game make you feel about your knowledge of cybersecurity?

(Select all that apply)

- ☒ Empowered
 - ☒ Informed
 - ☐ Confused
 - ☒ Motivated
 - ☐ Frustrated
 - ☐ Other:
-

21. Would you say your perception of cybersecurity has changed after playing the game?

- ☒ Yes

- ☐ No

- If yes, please explain: I have learn abt about Phishing and Safe browsing practice

22. Overall, how satisfied are you with your learning experience from the trivia twirl game?

- ☐ Very dissatisfied

- ☐ Dissatisfied

- ☐ Neutral

- ☐ Satisfied

- ☒ Very satisfied

Section 4: Experience with trivia twirl game

23. How would you rate your overall experience with the trivia twirl game?

- ☐ 1 (poor)

- ☐ 2 (Average)

- ☒ 3 (Excellent)

24. What aspects of the trivia twirl game did you find most engaging?

- ☐ Game Mechanics

- ☒ Question Variety

- ☐ Visual Design

- ☐ Interactive Experience

- ☐ Other (Please specify):

25. Did the trivia twirl game enhance your understanding of cybersecurity topics?

- ☒ Yes, significantly

- ☐ Yes, somewhat

- ☐ No change

- ☐ No, it confused me

Section 5: Attitudes Towards Gamification

26. Are you familiar with the concept of gamification in training?

- ☐ Yes
- ☒ No

27. On a scale of 1 to 5, how effective do you think gamified training methods would be for improving cybersecurity awareness?

- ☐ 1 (Minimum effective)
- ☐ 2 (Low effective)
- ☐ 3 (Moderate effective)
- ☒ 4 (High effective)
- ☐ 5 (Very high effective)

section 6: Implementation and Feedback

28. What challenges do you think the local government might face in implementing the trivia twirl game for cybersecurity training?

Lack of resources and poor Network, and shortage of IT personnel

29. How frequently should gamified cybersecurity training be conducted?

- ☒ Monthly
- ☐ Quarterly
- ☐ Bi-Annually
- ☐ Annually
- ☐ Other (Please specify): _____

30. Would you participate in regular sessions of the trivia twirl game to improve cybersecurity awareness?

- ☒ Yes
- ☐ No
- ☐ Maybe

31. What specific features or topics would you like to see included in future iterations of the trivia twirl game?

Data Protection

32. What additional resources or support would you need for effective gamification of cybersecurity training?

Tablet or laptops and Data, Technological resource,
Possible ways to stop hackers

Section 7: Final Thoughts

33. Please share any additional comments or suggestions regarding the use of the trivia twirl game for enhancing cybersecurity awareness in local government.

I Support the use of trivia twirl game. It attracts lots of attention, and ^{we gain} ~~gives~~ knowledge faster than reading Case Studies, Compulsory Course for all administration staff. Also using internet