Cybersecurity of information systems at the National Archives and Records Service of South Africa

Ntandoyenkosi Sinqobile Moyana[1] and Kabelo Given Chuma[2]
nmoyana@iie.ac.za ORCID: 0009- 0001-8130-7674
chumakg@unisa.ac.za ORCID: 0000-0002-5817-6063

Received: 5 February 2023
Accepted: 4 December 2023

In today's computerised world, cybersecurity attacks have become a major headache with detrimental effects on cultural institutions including libraries, archives, and museums around the world. The exponential growth in the use of Information and Communication Technology (ICT) and advances in digitalisation have increased the complexity of cybersecurity attacks and threats. Archival repositories face greater exposure to cybersecurity threats and attacks due to increasing digitalisation. In South Africa, a growing number of cultural heritage institutions such as archival repositories and libraries are under constant attack by cybersecurity threats and attacks to disrupt systems, networks, and services offered to the citizens. Cybersecurity could serve as the wall keeping malicious actors from attacking these institutions. This qualitative study sought to explore cybersecurity of information systems at the National Archives and Records Service of South Africa (NARSSA) in Pretoria. Data were collected through semi-structured interviews that were tape-recorded and analysed using a thematic analysis and NVivo 12 software package. The findings of this study revealed that the NARSSA is under severe attack from phishing attacks, computer viruses and worms, Trojan horses, password attacks, and Denial of Service attacks. The results further showed that Microsoft firewall, audit train, strong user password and anti-virus software were put in place to mitigate cybersecurity attacks and threats. The NARSSA should achieve a strong cyber resilience security posture to protect computer systems against cyber-attacks. It is concluded that the NARSSA needs to invest heavily in a security awareness program to continually train staff on how to identify and respond appropriately to the growing range of cyber security threats and defend against attacks such as phishing attacks, social engineering attacks, ransomware attacks, and malware attacks.

Keywords: cybersecurity, cyber-attacks, computer security, information systems, security techniques, National Archives of South Africa

1 Introduction and background to the study

The use of Information and Communication Technology (ICT) is pervasive in many public institutions today. The rapidly evolving ICT has substantially transformed public heritage organisations including archives, historical sites, libraries, and museums. According to Ioannidis, Toli, Raheb and Boile (2014), the integration of ICT has significantly changed how cultural heritage institutions operate, particularly, concerning records management. The advent of these technologies has accelerated the creation of electronic records, which are essential for modern organisations, especially archives. Nyampong (2015) and Masenya and Ngulube (2021) affirm that the growing use of ICT in government has accelerated the generation of electronic records, which are essential to the function of public sector institutions. In contrast, Xu, David & Kim (2018) assert that the advancement in ICTs has brought the entrance of digital records, which are created and managed using a computer or machine-readable device in archival institutions and/or records organisations (Xu, David & Kim 2018). Krishna and Sebastian (2021), further state that technology is crucial for the development of nations. Consequently, ICTs have recently been embraced by many archival institutions across the globe to better enhance and coordinate their day-to-day operations and records management processes. Zazzau (2007) attests that archival repositories embrace new digital technologies to facilitate better access to and retrieval of information and archival materials.

According to Krubu and Osawaru (2011), archival institutions around the world use a range of ICTs to provide consumers with value-added information services and access to a wide range of digitally based resources. Despite the advent of new technologies used in archival practice, there has been a phenomenal growth of cyber-attacks and threats facing archival institutions. According to Oyedum, Sanni and Udoakang (2014) and Shafack (2021) the continuous growth of electronic data and extensive use of digital technologies in libraries, archives, and records management has resulted in an influx of cyber-attacks and threats. Furthermore, recent literature on archival and records management security revealed

1. Ntandoyenkosi Sinqobile Moyana is Librarian at the Independent Institute of Education in South Africa
2. Kabelo Given Chuma is Lecturer in the Department of Information Science at the University of South Africa

that as digital technologies become more widely used in archival institutions and records organisations, they pose new challenges for computer security and electronic archival records (Donaldson & Bell 2018). The most prevalent cyber-attacks facing archival institutions include malware and phishing attempts, data breaches, trojan horses, ransomware, and email hijacking. McHugh (2022) affirms that security threats in archives and records management are diverse and include malware, phishing, ransomware, data breaches, and theft, making it essential to incorporate multiple forms of security.

The Archives and Records Association in the United Kingdom reported that many archives in the United States and the United Kingdom were increasingly under attack by malware, phishing, and data breaches amidst the COVID-19 pandemic, resulting in the vulnerability of archives services and disruptions in the delivery of public information and tasks. These cybersecurity attacks originate from various sources including espionage, industrial spies, terrorism, critical infrastructure sabotage, and organised crime groups (Enoksen & Söderholm 2018; Li & Liu 2021). Consequently, these attacks often cause damage to computer systems while affecting the spectrum of archives services and the application domains simultaneously. The South African public sector has become a prime target for cybercriminals and is vulnerable to cyberattacks, largely because they are becoming more digitally mature, their wheels turn slowly, and many are overburdened and under-resourced, especially when it comes to cybersecurity. Prasad (2022) attests that the South African public sector has become a target for cybercriminals and attacks, which threaten the economy, people, infrastructure, and organisation (Ngoma, Keevy & Rama 2021). Amid the COVID-19 pandemic, several public sector organisations, including archival institutions and libraries, experienced an increase in cyber-attacks detected by their servers.

According to Keevy and Rama (2021), government departments, and public entities like archival repositories, libraries and business institutions have been plagued with cybersecurity threats and attacks resulting from outdated legislation, obsolete systems and equipment, and poor infrastructure. Given this context, the security of digital collections held by archival institutions is a legitimate concern. Thus, South African archival institutions need to ensure the protection of the confidentiality, integrity, and availability of their systems and records. In light of the current issues of cybersecurity, there is a critical need to develop the technical and institutional capabilities within archival institutions to respond to emerging cybersecurity threats and attacks triggered by digital technologies. Therefore, this study sought to explore cybersecurity of information systems at the National Archives and Records NARSSA in Pretoria.

2 Problem statement

National archives repositories play the most significant role in the preservation of a nation's history and its citizens' rights. According to Sibhidla-Saphetha (2013), archival institutions have an essential role to play in the preservation of the culture and national heritage of the country. As part of their responsibilities, national archives are charged with preserving and providing access to records of the government, departments, agencies, and institutions (Venson, Ngoepe & Ngulube 2014; Netshakhuma 2019). They are engaged in conducting their public business to protect their records against cyber threats and attacks, regardless of the format of the records. These records contain the most confidential and sensitive information pertaining to the actions and decisions of government, institutions, communities and historical foundation of the state and its citizens. Due to the sensitive nature of the information contained in archival records, ensuring the security of records and computer systems is an integral part of building the trust required to realize the potential benefits of using new technologies in archival institutions.

Ngoepe, Mokoena and Ngulube (2010) argue that archival collections and records require basic security to ensure their integrity and authenticity, as well as to prevent misuse and unauthorized access. It is vital that archival repositories mitigate cyberattacks against computer systems and set up protections that allow access to archival materials while ensuring that they are protected to the fullest extent possible. The overarching problem that fuelled this study is that the NARSSA is facing a quadruple burden of security challenges emerging from the increasing use of new technologies. Sithole (2019) affirms that public sector organisations in South Africa are facing security challenges arising from the use of electronic records and computer systems. In response to observations and frequent requests for assistance by staff, it was established that the NARSSA struggles to fully protect computer systems and archival materials from a diverse range of cybersecurity attacks. It was assumed that the NARSSA staff could be experiencing inappropriate protection measures in place to prevent these emerging threats and attacks.

The NARSSA has made substantial efforts to enhance the security of computer systems and reduce the risks of cyber-attacks. This includes updating defensive practices as well as developing effective security strategies to enhance the security of computer systems. Despite the considerable efforts by NARSSA, there are still occurring incidents relating to cybersecurity attacks that threaten the confidentiality, integrity, and availability of computer systems.

3 Research purpose and objectives

The purpose of this study was to explore the cybersecurity of information systems at the NARSSA in Pretoria. To achieve the above-mentioned purpose, the following research objective were set:

- To analyse legal frameworks governing the cybersecurity of computer systems in the NARSSA in Pretoria.
- To examine the cyber-attacks threatening computer systems in the NARSSA in Pretoria.
- To determine the motivations behind cyber-attacks plaguing computer systems in the NARSSA in Pretoria.
- To establish the security techniques for securing computer systems against cyber-attacks in the NARSSA in Pretoria.
- To recommend the strategies that can be implemented to prevent and detect cyber-attacks facing the NARSSA in Pretoria.

4 Conceptual framework of the study

The conceptual framework refers to the overall, logical organization and association of everything that forms the underlying thinking, structure, plans, practices, and implementation of your whole research project. According to Ravitch and Riggan 2017), a conceptual framework describes how you identify the research topic, what you intend to investigate, what questions you intend to ask, what literature to review, what theories you intend to apply, how you will conduct the research, what methods and procedures you will use, how you will interpret and analyze your data, and what recommendations and conclusions you will make.

For the purpose of this study, the researchers developed a conceptual framework which was informed by the literature and Routine Activity Theory (RAT) to conceptualise the nature of their research problem (Salmons 2019) and provide a clear and concise understanding of the key concepts, variables, relationships, and assumptions that underlie a research study. The proposed conceptual framework includes the following key constructs: (a) legal frameworks, (b) cyber-attacks, (c) motivations, and (d) security techniques. Figure 1 illustrates the conceptual framework of the study.

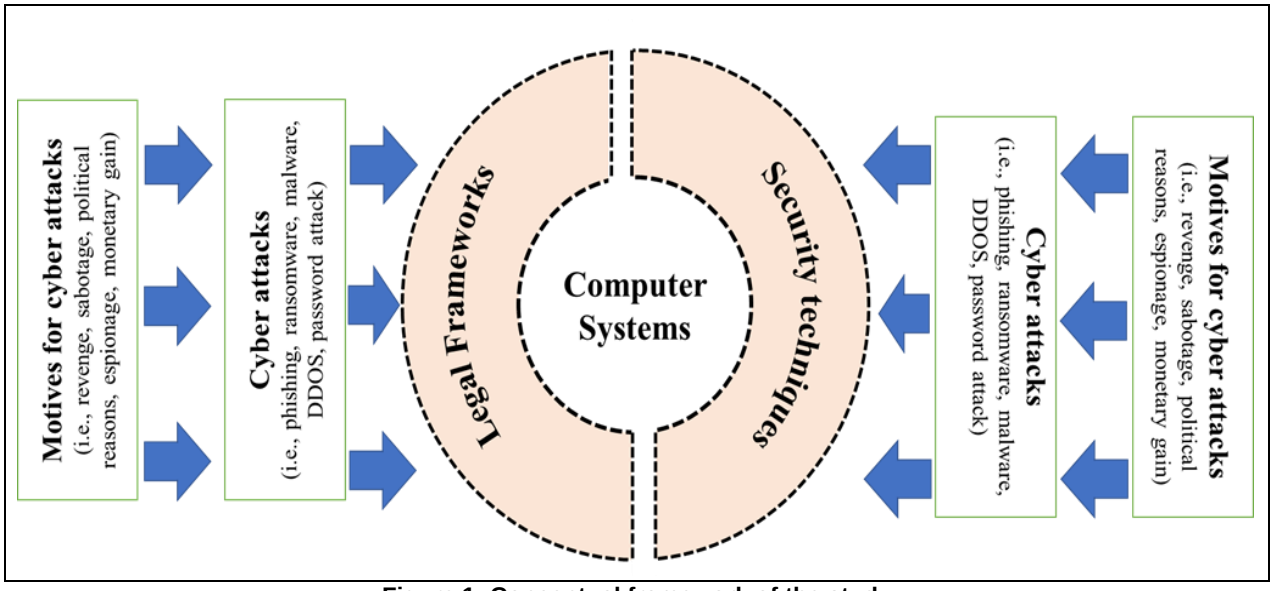

Figure 1: Conceptual framework of the study

In developing the conceptual framework, the researchers used critical concepts from the RAT, including motives for cyber-attacks and security techniques. RAT is an analytical framework that has been well-tested and innovative, making it adaptable to law enforcement use. This theory has been successful in understanding the factors influencing cybercrimes in organisations (Leukfeldt & Yar 2016). Cybercrime is generally used broadly to describe criminal activities that involve the use of technologies such as a computer or networked devices to facilitate crimes like data theft or financial fraud. Donalds and Osei-Bryson (2019) define cybercriminal as an act, crime, or illicit conduct committed against a computer, computer-related device, and/or a network of information technology considered a cybercrime, as well as traditional crimes that are facilitated or maintained through the use of the internet and/or information technology. The theory comprises three integral components including a suitable target, the absence of a capable guardian, and a likely or motivated offender.

The 'likely offender' refers to those attackers who exploit the current opportune situation by choosing more online users as their 'suitable targets', while the 'guardian' refers to the security measures in place to protect online users. These key

components are applied in the context of the online environment. Yar (2005) advocates that RAT provides a macro perspective to understand various cyberattacks launched by offenders or cyber actors and their motivations to commit cybercrimes. The theory provided researchers with a conceptual foundation for understanding the most prevalent cyber-attacks targeting computer systems at NARSSA. The theory also enabled the researchers to understand the motivations that inspire cyber actors to cyber-attacks in NARSSA. A suitable target is a person or property that may be threatened by an offender (Felson & Clarke 1998). Given this context, archival institutions are suitable targets because they are official custodians of the records of the enduring value of the government and people's collective memory.

Consequently, this is likely to motivate offenders to target governments, organisations, and institutions. Researchers were able to gain insight into why archival institutions are targeted by cybercriminals through applying the RAT. Guardians capable of preventing crime are those whose presence prevents crimes from happening, and whose absence increases their likelihood (Felson 1995). Govender, Watson and Amra (2021) stress that capable guardians are end users that are capable of using security control measures such as firewalls, anti-virus and anti-intrusion software and access management to mitigate cybersecurity attacks. Through the use of the RAT, researchers were able to examine the security control measures in place at NARSSA to prevent cyber-attacks. According to RAT, the impact of capable guardianship is the most important factor in reducing victimisation (Leukfeldt & Yar 2016).

5 Review of the related literature

This section presents the literature review to address the research objectives of the study.

5.1 Legal frameworks for cybersecurity in South Africa

An efficient legal framework is the first step toward good computer security governance. Public institutions all over the world require comprehensive legal and regulatory frameworks to regulate the processing of any data and adequately address how data is stored, disseminated, and protected in computer systems. According to Šimundic, Boban and Šinković (2010), legal and regulatory frameworks are essential in public organisations to protect the right of access to information and data stored in computer systems and make it available under any circumstances. As digital technologies become more prevalent, large institutions with computerised databases of records as well as surveillance capabilities of computer systems require legislation and regulations governing data and system protection. Thus, they are expected to implement and enforce compliance with regulatory requirements to ensure that records and systems are properly secured and protected over time. Hamooya, Mulauzi and Njobvu (2011) concur that legal and regulatory frameworks are vital to the effective management of records and archives throughout their lifecycle. They provide a framework within which archival and records management systems can be implemented and protected.

South Africa has enacted several pieces of legislation to protect data and computer systems within organisations and institutions (Baloyi & Kotzé 2017; De Bruyn 2014). The most relevant legislation dealing with the protection of data and systems in public organisations include the Promotion of Access to Information Act 2 of 2000, Electronic Communications and Transactions Act 25 of 2002, the Protection of Personal Information Act 4 of 2013, the Constitution of the Republic of South Africa Act 44 of 1995, Promotion of Administrative Justice Act 3 of 2000, and Cybercrimes and Cybersecurity Act of 2017 (South African Government Gazette 2013, Department of Justice and Constitutional Development 2017). These pieces of legislation establish the rights to protect staff members against misuse of records and obligations that require archival institutions to use computer systems fairly, transparently, and responsibly to build trust in archival institutions and society. It essential for public entities such as archives to ensure strict adherence to legal requirements because any failure to comply with regulations may result in potential consequences such as legal penalties, financial forfeiture, damaged reputation, and material loss.

In South Africa, there are several policy manuals established by the government to provide a foundation of directives, rules, and practices that define how government departments, organisations, companies, and institutions can manage, secure data and systems, and detect cyber threats. Some of the most common policies include European Union Agency for Network and Information Security (ENISA), National Cybersecurity Policy Framework, Cybercrimes and Cybersecurity Bill (Department of Justice 2015). The purpose of these policies is to properly handle cybercrimes and enforce security in organisation.

5.2 Cybersecurity attacks threatening computer systems

Cybersecurity attacks have become a global and complex problem targeting and harming many sectors, industries, governments, and organisations across the world, particularly those relying on technologies. According to Shu, Sliva, Sampson and Liu (2018), there has been an increase in cyberattacks affecting individuals, businesses, and society as a whole. A cyber-attack is thus a term properly used only to refer to a malicious and deliberate attempt to gain unauthorized

access to alter a computer system and/or network with the intention to cause damage or harm. According to Fayomi, Ndubisi, Ayo, Chidozie, Ajayi and Okorie (2015), the term cyber-attack has been widely acknowledged as “an attempt by hackers to damage or destroy a computer network or system for purposes of mischief, fraud, and/or hedonism”. There are various types of cyber-attacks affecting many nation states and public organisations (Silva 2020). The literature review revealed that cybersecurity attacks such as malware attacks, phishing attacks, social engineering, web-based attacks, and IoT-Based attacks are causing extensive damage to corporate sectors, government organisations and computer systems (Sithole 2019, Toapanta, Cobeña & Gallegos 2020).

Governments, businesses, organisations**,** and most importantly their systems and infrastructure are exposed to cyber-attacks such as eavesdropping attacks, password attacks, Man-in-the-middle (MitM) attacks, SQL injection attacks, Drive-by-download attacks, cross-site scripting attacks, File Inclusion attacks (Fayomi, Ndubisi, Ayo, Chidozie, Ajayi & Okorie 2015). Archival storage systems are exposed to a host of cybersecurity threats including long-term secrecy, poor, or missing authentication schemes, and slow attacks. These security threats may endanger the secrecy, availability, and integrity of the archival records. Furthermore, a recent study by Donaldson and Bell (2018) revealed that digital collection and computer systems in archival institutions are highly vulnerable to security breaches, malicious insiders, viruses, phishing attempts, malware, and denial of service attacks. Curtis and Wright (2021) attest that archival repositories in Australia are facing a myriad of cyber-related attacks including malware, phishing, ransomware, insider attacks, Trojans, and breaches. These cyber-attacks can cause significant damage to computer systems and disrupt archival services.

5.3 Motives behind cyber-attacks in organisations

A good understanding of motivation is crucial to identifying the attacker's goals, methods, victims, and capabilities. Cybercriminals with malicious intentions have many motives for launching cybersecurity attacks in order to gain unauthorised access to computer systems in organisations. Li (2017) affirm that malicious actors have various motivations when launching cybersecurity attacks to gain unauthorised access to computer systems. According to the literature reviewed, the most fundamental motivations or reasons behind cybersecurity attacks intended to cause harm or damage to computer systems include profit or financial gain and espionage, social or political point, revenge, sabotage, and extortion (Li 2017, Chng, Lu, Kumar & Yau 2022). Chuma and Ngoepe (2022) stress that malicious actors are highly motivated by financial profit, political gain, sabotage, and espionage to penetrate computer systems and networks.

According to Gandhi, Sharma, Mahoney, Sousan, Zhu and Laplante (2011), there are three categories of motivation for cyber-attacks including (i) political motivations (i.e., destroying, disruptions, espionage, and retaliatory actions), (ii) economic motivations (i.e., sabotage, financial gain, blackmail, fraud, and industrial espionage), and socio-cultural motivations (i.e., fun, curiosity, ego gratification, and publicity). Given this context, archival collections contain the most sensitive, classified, or personal information which may be of use to cybercriminals. Consequently, cybercriminals may use this motive to attack archival institutions. Figure 2. illustrates different types of cyber threat actors and their motivations.

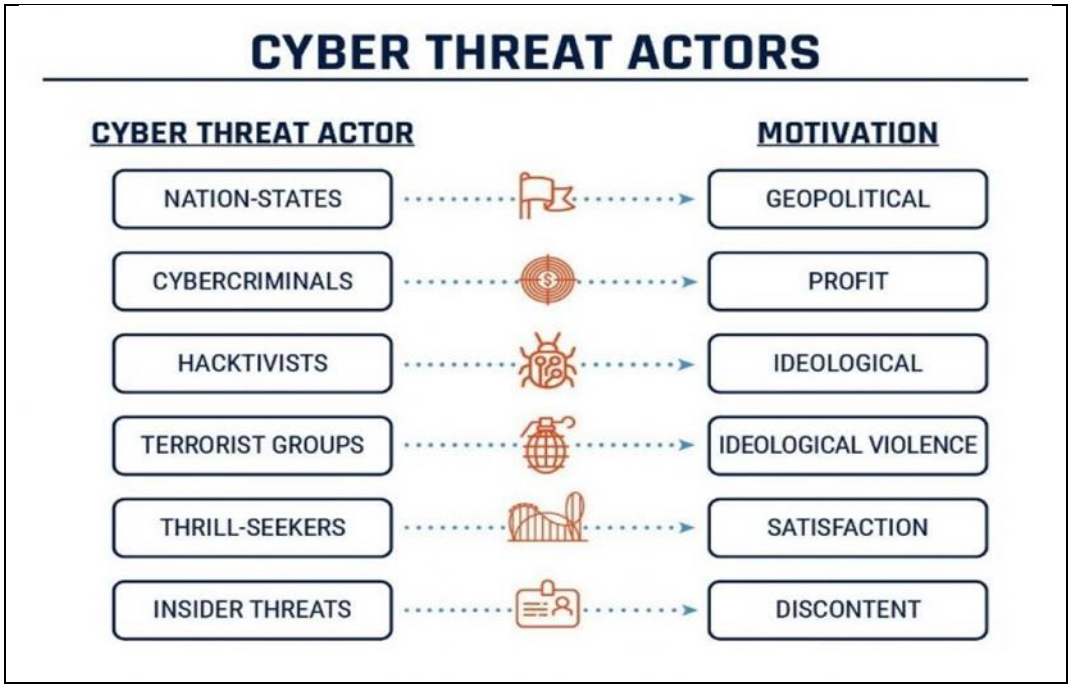

Figure 2: Cyber actors and their motivations (NI Cyber Security Centre 2020)

5.4 Security Techniques for Securing Computer Systems against Cyber-Attacks

Archival institutions must put in place security measures or precautions to protect computer systems against cybersecurity attacks. According to Donaldson and Bell (2018), libraries and archival institutions are often connected to larger institutions, such as universities; therefore, they need to take necessary security measures to protect computer systems and networks. Security mechanisms such as data encryption, use of strong passwords, control access to systems, anti-virus computer software, Microsoft firewalls, and Intrusion Detections System can be used by organisations to protect and secure data, computer systems and networks against possible cyber threats and attacks (Jakimoski 2016; Liao 2017).

An empirical study conducted by Donaldson and Bell (2018) indicated that staff should use strong passwords to ensure the security of digital collections, ensure that computer systems are patched and updated, and back up all personal computer data to an alternate hard drive or server to prevent data loss and unauthorized access to archives and library systems. Furthermore, archival institutions must develop, implement, and enforce security policies and procedures to regulate and control access to digital collections, objects, and digital data and prevent unauthorized access to archives systems.

6 Research methodology

The study was situated within the interpretivism paradigm. Due to the interpretive and exploratory nature of the study, the qualitative research approach was applied to capture in-depth and detailed explanatory data on perspectives and understandings of cyber-attacks threatening computer systems in the National Archives and Records Service of South Africa in Pretoria. The use of a qualitative research approach enabled the researcher to gain insight into the natural context of the participants and empowered the participants by giving them a voice in the study (Creswell 2013). A case study research design was employed to identify issues and problems associated with cybersecurity attacks, which have not been extensively studied yet. The target population for this study comprised of Record Managers, Records Clerks, and IT Specialists currently employed in NARSSA. The study employed a purposive sampling technique to select participants. According to Etikan, Musa and Alkassim (2016), a purposeful sampling technique (also called judgment or subjective sampling) is the deliberate selection of participants based on their characteristics.

In this technique, there is no need for underlying theories or a set number of participants. To put it simply, the researcher determines what information is needed and sets out to find people with knowledge or experience who can and will provide it (Bernard 2002). Through the use of this sampling technique, researchers were able to collect qualitative responses, resulting in more precise and insightful research findings about cybersecurity attacks on computer systems in the NARSSA. Data was gathered using semi-structured interviews with selected study participants. This technique offered researchers the freedom to explore any pertinent thoughts that arose throughout the interview. Furthermore, thematic analysis was used to analyse qualitative data collected through interviews. Dawadi (2021). Thematic analysis is a qualitative research method used to systematically organise and analyze complex data sets. In this technique, narratives are captured in the account of data sets through the use of themes. Consequently, this technique was used to identify patterns and themes and interpret the data (Braun & Clarke 2012). The NVivo 12 software was used to organise, analyse and visualising the qualitative data of this study.

7 Findings of the study

This section of the study presents the findings in accordance with themes emerged from the research objectives.

7.1 Legal framework governing the cybersecurity of computer systems in NARSSA

Legal and regulatory frameworks include guidelines and best practices that organisations must follow to comply with a variety of security requirements. They are enacted by governments to specify certain standards of behavior for individuals, corporations, or other entities. Laws are the mandatory national directives that a utility must adhere to when it comes to cybersecurity. The purpose of legal and regulatory frameworks is to guide organisations in protecting their systems and relevant information and data Participants were asked to share their knowledge of existing legislation for that govern cybersecurity of computer security in NARSSA. Figure 3 illustrates several pieces of legislation mentioned by the participants during the interviews.

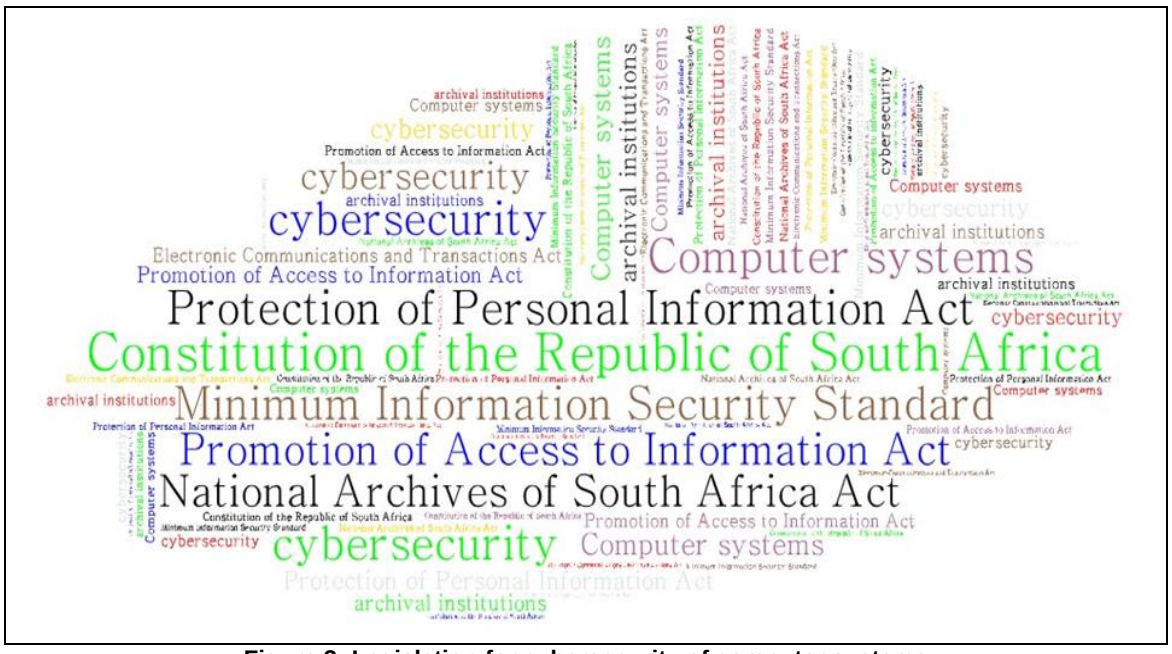

Figure 3: Legislation for cybersecurity of computer systems

For example, participant (AC1) said:

> *The National Archives of South Africa has taken significant steps to implement laws and regulations relating to the protection of archival data and records stored in computer systems. Just to mention a few, some of the most common laws implemented in our archives include the Constitution of the Republic of South Africa, Electronic Communications and Transactions Act, and Protection of Personal Information Act, 2013. It is important for us to maintain strict compliance with these regulatory requirements to ensure that our systems are well maintained and protected in accordance with the guidelines that are stipulated in these legislation and laws.*

Another participant (AC3) mentioned that:

> *We have incorporated several pieces of legislation and regulations that are essential for maintaining and securing the integrity, privacy and trustworthiness of our computer systems and availability of data, which include Protection of Personal Information Act, 2013, Promotion of Access to Information Act 2 of 2000, Minimum Information Security Standard, Electronic Communications and Transactions Act, National Archives of South Africa Act and Constitution of the Republic of South Africa. Although other regulations exist, these are a few of the ones I can think of that we have adapted to meet the evolving security requirements in order to protect our archival data and computer systems.*

Security policies are an essential component of an information security program, and need to be properly crafted, implemented, and enforced. As a follow up question, participants were asked whether they have a security policy that spells out the rules, guidelines, and overall approach that the National Archives uses to maintain the confidentiality and integrity of computer systems. During the interviews, participants disclosed that the National archives has not put in place any security policy that provide technical guidance to protect data and computer system. For example, participant (AC5) indicated that:

> *In the National Archives, we do not have documented security policies and procedures that govern the computer security. As a precaution, we have Standard Operation Procedures (SOPs) in place for ensuring the security and protection of our computer systems. These SOPs are useful for providing steps and standardised procedures for managing and protecting data and computers. Additionally, these SOPs guide our staff members on how they must comply with South African data protection laws.*

7.2 Cyber-attacks threatening computer Systems in the NARSSA

Sharma and Purohit (2018) argue that cybersecurity attacks and threats are becoming more common, sophisticated, and prevalent for organisations dealing with the most sensitive and confidential information. National archives are particularly vulnerable and targeted by cyberattacks because they possess so much information of high monetary and intelligence value to cyber thieves and nation-state actors.

Zetter (2018) affirms that the sensitive and confidential information that is held by libraries, archives and museums has made them prime targets for cybercriminals over recent years, given the sensitive nature of their collections. Participants were asked to share their knowledge based on cybersecurity threats and attacks facing computer systems in the NARSSA. Figure 4 shows cyber-attacks and threats identified by participants during the course of the interviews:

Figure 4: Cyber-attacks and threats in the NARSSA

For example, Participant (AC8) said:

> *We usually experience a great number of cyber-attacks especially since the beginning of the COVID-19 pandemic in South Africa. Some of the most common cyber-attacks we have encountered here at NARSSA is phishing attacks through our work emails, password attacks and trojan horses. And, on a daily basis, we frequently experience computer viruses and worms. I think this is because people are using USBs and external hard drives in computers. So, this is some of the security threats we often experience.*

Another participant (AC2) offered a similar response and alluded that:

> *The most cyber-attacks we often experience from our computers is Trojan horses, email phishing attacks, viruses from USBs, and denial of services. As a result of these cyber-attacks, our computer systems are often affected by serious problems that result in our computer systems being slower and malfunctioning often because of the cyber-attacks.*

Participant (AC4) also indicated that:

> *Ok. Some of the security threats that we encounter on a daily basis in the National Archives of South Africa include password attacks launched through a network protocol, computer viruses, phishing attacks via links sent in emails, and worms. These are among the threats and attacks I can recall. But we always find a way to deal with these threats to avoid severe any damages or disruptions to our computer systems.*

7.3 Motivations behind cyber-attacks and threats in the NARSSA

There is a growing need for public organisations like archives to understand the motivations that incite cyber-attacks and determine cyber risks as a means for curbing and responding to emerging cyber-attacks. Han and Dongre (2014) affirm

that understanding cyber threat agents' motivations, strategic considerations, as well as their attack methods, can aid organizations in responding to cybersecurity threats. Consequently, understanding cyber threat actors and their motivations is crucial for identifying cyber incidents and reducing their impact.

In contrast, Han and Dongre (2014) argue that knowing the existing threat to cyber security is fundamental to understanding the motivations for cyber attackers. A better understanding of different motives for cyber threat actors contributes to higher level of maturity in cyber threat detection. As part of the study, participants were asked to reflect on the motivations behind cybersecurity threats and attacks that NARSSA is experiencing. Figure 5 shows the responses from participants about the motivations for cyber-attacks in NARSSA.

Figure 5: Motives behind cyber attacks and threats in NARSSA

For example, participant (AC10) said:

> *It is important to reflect that the National Archives is responsible for collecting and holding that most sensitive information, archival films, and video collections that contain the most significant monetary and historical value. I personally think that cybercriminals are highly motivated to launch cyber-attacks for financial gain, political power, and espionage. These people they know that these collections can generate money for them, so they have the motive to launch these threats.*

Another participant (AC1) stipulated that:

> *I think cybercriminals and hackers are primarily motivated by financial gain, espionage, and sabotage to attack the National Archives of South Africa because of its valuable collections and material in the custody.*

In a follow-up question, participants were asked who they believed was responsible for launching these security threats against the National Archives. Participant (AC5) said:

> *The most cybercrimes happening in the National archives of South Africa are committed by hacktivists, cybercriminals, and hackers who are desperate to make money out of archival holdings and collections.*

7.4 Security techniques for protecting computer systems in the NARSSA

The importance of cybersecurity in organisations cannot be overemphasised. Archival records are considered the most important assets of any archival institution. With that in mind, archival institutions should take appropriate security measures to protect their computer systems and information from cyber-attacks, to ensure business continuity, and to provide uninterrupted archival services. According to Lenaeus, O'Neil, Leitch, Glantz, Landine, Bryant, Lewis, Mathers, Rodger and Johnson (2015), security control measures play the most significant role in protecting information, computer systems and networks against theft, vandalism, invasion of privacy, unauthorised access or modification and other irresponsible behaviours.

Participants were asked to share their knowledge about the security techniques which have been put in place in the NARSSA to protect computer systems against cyber-attacks and threats. Figure 6 shows the security techniques indicated by participants during the interviews.

For instance, participant (AC4) alluded that:

> *In the National Archive we use several security techniques to prevent cyber-attacks and threats from happening. We use the Microsoft firewall, password, and username, as well as the audit trail system to detect and trace any movement within our computer systems. We rely on these techniques to protect archival data captured in our systems.*

Participant (AC2) said:

> *We have installed the anti-virus software in all the computer systems to prevent any viruses and worms from USBs and we always ensure the Microsoft firewall is turned on to prevent cyber-attacks like phishing and Trojan horses. However, the challenge that we have is that we do not regularly update the anti-virus, Firewall and Windows Operating Systems. As a result, this makes our computer vulnerable to cyber-attacks and threats. But it is something that we will work on to improve the security of our computer systems.*

8 Discussion of the findings

This section discusses the research findings in accordance with themes derived from research objectives.

8.1 Legal framework governing the cybersecurity of computer systems in the NARSSA

The findings of the study demonstrated that the Minimum Information Security Standard, the Promotion of Access to Information Act, 2 of 2000, the Protection of Personal Information Act, Constitution of the Republic of South Africa, 1996, Electronic Communications and Transactions Act 25 of 2002 and the National Archives of South Africa Act (No. 43 of 1996) are among pieces of legislation that NARSSA uses to protect its information and systems from abuse. These regulations have been established to safeguard computer information systems against cyber-attacks; therefore, any organisation in South Africa needs to ensure strict adherence to these regulations (Department of Justice and Correctional Services 2017; Roos 2016; Gallens 2016).

Furthermore, it was found that the NARSSA does not have documented security policies and procedures that adequately deal with computer security. Based on the results of the study, it is clear that NARSSA has implemented SOPs that guide its staff in relation to computer security

8.2 Cyber-attacks threatening computer systems in the NARSSA

The findings of this study showed that the NARSSA is confronted with a variety of cybersecurity threats and attacks including phishing attacks, computer viruses and worms, Trojan horse, password attacks, and Denial of Service attacks (DOS and DDoS), which result in severe consequences. Masombuka, Grobler and Duvenage (2021) affirm that vast majority of government institutions and entities are exposed to a variety of cybersecurity threats and attacks such as computer worms, phishing, Trojan horse, and computer viruses.

These cybersecurity threats and attacks has the potential to cause probable damage/disruption to the information and computer systems.

8.3 Motivations behind cyber-attacks and threats in the NARSSA

According to the study findings, espionage, sabotage, political and financial gains, and espionage were identified as the most common motivations behind cyber-attacks and threats faced by NARSSA. A study conducted by Kaiser, Wiens and Schultmann (2021) discovered that cybercriminals, hacktivists, and hackers are motivated by espionage, self-expression, curiosity, financial gains, social acceptance, and ideological to launch cyber-attacks to organisations.

The study also revealed that NARSSA has extensive archival film and video collections that have significant monetary and historical value, driving cyber threat agents to launch cybersecurity threats and attacks to computer systems. Moreover, it was found that hacktivists, cybercriminals, and hackers were primarily responsible for the majority of cyber-attacks threatening computer systems in the NARSSA.

8.4 Security techniques for protecting computer systems in the NARSSA

With regards to security measures used in the NARSSA, the results showed that Microsoft firewall, audit train, strong user password and anti-virus software were put in place to protect electronic records and computer systems against emerging cyber-attacks and threats. However, it was disclosed from the interviews that IT staff in the NARSSA do not routinely update the anti-virus software, Firewall and Windows Operating Systems (OS). Choudhary, Saroha and Beniwal (2013) stress that outdated antivirus software, firewall misconfigurations and out-of-date Operating Systems can allow malware infections to impact the computer systems.

9 Conclusion and recommendations

The purpose of the current study was to explore the cybersecurity of computer systems in the NARSSA in Pretoria. The results revealed several pieces of legislation implemented in NARSSA for the cybersecurity of computer systems including the Minimum Information Security Standard (MISS), the Promotion of Access to Information Act, 2 of 2000, the Protection of Personal Information Act, Constitution of the Republic of South Africa, 1996, Electronic Communications and Transactions Act 25 of 2002, and the National Archives of South Africa Act (No. 43 of 1996). The study discovered the absence of a security policy to address the cybersecurity of computer systems in NARSSA. This study further revealed a number of cyber-attacks facing the NARSSA including phishing attacks, computer viruses and worms, Trojan horses, password attacks, and Denial of Service attacks (DOS and DDoS).

Furthermore, it was clear from this study that the motives behind cyber-attacks and threats facing NARSS include espionage, sabotage, and political and financial gain. Security control measures such as Microsoft Defender Firewall, security audit trail, strong username and password and anti-virus software were used in NARSSA to protect computer systems against cybersecurity attacks. It is important for the NARSSA to invest heavily in a security awareness program to continually train staff on how to identify and respond appropriately to the growing range of cyber security threats and defend against attacks such as phishing attacks, social engineering attacks, ransomware attacks, and malware attacks.

Based on the research results, the following recommendations might help to address cyber-attacks and improve the security of computer system in NARSSA:

- The study showed several pieces of legislation implemented in the NARSSA including Minimum Information Security Standard, the Promotion of Access to Information Act, 2 of 2000, the Protection of Personal Information Act, Electronic Communications and Transactions Act 25 of 2002, Constitution of the Republic of South Africa, 1996, and the National Archives of South Africa Act (No. 43 of 1996). Thus, the study recommends the need for NARSSA to incorporate several pieces of legislation for cybersecurity including the Cybercrimes Act 19 of 2020, National Cybersecurity Policy Framework, State Information Technology Agency Act 88 of 1998, Consumer Protection Act of 2008 and the Critical Infrastructure Protection Act (CIPA) 8 of 2019. These acts aimed at addressing cybercriminal activities and to provide for measures to be put in place for the protection, safeguarding and resilience of computer systems.

- The study revealed a lack of security policy and procedures in the NARSAA to address cyber-attacks. It is therefore recommended that NARSSA must establish an up-to-date cyber security policy that is in line with international standards to address cybersecurity threats and attacks, mitigate vulnerabilities, and restrict access to computer systems.
- The results of the study indicated that IT staff at NARSSA do not routinely update anti-virus software and Windows OS. Thus, the study recommends the need for IT staff to update the antivirus software and Windows OS regularly to patch security flaws and fix bugs.
- The NARSAA should use data encryption and decryption to secure and protect digital records as they are stored on computer systems and transmitted through the Internet.
- The study suggests the need for NARSSA to achieve a strong cyber resilience security posture to detect, respond to, and recover from cybersecurity threats and attacks.

References

Baloyi, N. and Kotzé, P. 2017, May. Are organisations in South Africa ready to comply with personal data protection or privacy legislation and regulations? In *2017 IST-Africa Week Conference (IST-Africa*) (pp. 1-11). IEEE.

Bernard, H.R. 2002. *Research methods in anthropology: qualitative and quantitative approaches*. (3rd ed.). Walnut Creek, CA: Alta Mira Press.

Braun, V. and Clarke, V. 2012. Thematic analysis. In H. Cooper, P. M. Camic, D. L. Long, A. T. Panter, D. Rindskopf, & K. J. Sher (Eds), *APA handbook of research methods in psychology, Vol. 2: Research designs: Quantitative, qualitative, neuropsychological, and biological* (pp. 57-71). Washington, DC: American Psychological Association.

Chng, S, Lu, H.Y, Kumar, A. and Yau, D. 2022. Hacker types, motivations, and strategies: a comprehensive framework. Computers in Human Behavior Reports, 5: p.100167.

Choudhary, S, Saroha, R and Beniwal, M.S. 2013. How anti-virus software works? *International Journal*, 3(4): 483-484

Chuma, K.G. and Ngoepe, M. 2022. Security of electronic personal health information in a public hospital in South Africa. *Information Security Journal: A Global Perspective*, 31(2): 179-195.

Cohen L.E. and Felson M. 1979. Social change and crime rate trends: a routine activity approach. *American Sociological Review,* 44 588–608.

Curtis, K. and Wright, S. 2021. Archives at risk of cyber-attack, security expert warns. [Online] https://www.smh.com.au/politics/federal/archives-at-risk-of-cyber-attack-security-expert-warns-20210628-p584ts.html (Accessed 2 October 2022)

Dawadi, S. 2021. Thematic analysis approach: A step by step guide for ELT research practitioners*. Journal of NELTA*, 25(1-2): 62-71.

De Bruyn, M. 2014. The protection of personal information (POPI) act: impact on South Africa. *International Business and Economic Research Journal,* 13(6): 1315-1350. DOI https://doi.org/10.19030/iber.v13i6.8922

Department of Justice and Correctional Services. 2017. *Cybercrimes and Cybersecurity Bill*. Pretoria: Government Printers.

Department of Justice. 2015. *Cyber Crime and Cybersecurity Bill*. Pretoria: Government Printers.

Department of Justice and Constitutional Development. 2017. *South African Banking Risk Information Centre (SABRIC)*. Pretoria: Government Printers.

Donalds, C. and Osei-Bryson, K.M. 2019. Toward a cybercrime classification ontology: a knowledge-based approach. *Computer Human Behaviour*, 92: 403–418.

Donaldson, D.R. and Bell, L. 2018. Security, archivists, and digital collections. *Journal of Archival Organization*, 15(1-2): 1-19.

Etikan, I, Musa, S.A and Alkassim, R.S. 2016. Comparison of convenience sampling and purposive sampling. *American Journal of Theoretical and Applied Statistics*, 5(1):1-4.

Fayomi, O, Ndubisi, O.N, Ayo, C, Chidozie, F, Ajayi, L. and Okorie, U. 2015. Cyber-attack as a menace to effective governance in Nigeria. In Proceedings of the 15th European Conference on eGovernment ECEG 2015 University of Portsmouth (p. 107).

Felson, M. and Clarke, R.V. 1998. *Opportunity makes the thief. Practical theory for crime prevention (Police Research Series, Paper 98)*. London: Home Office, Policing and Reducing Crime Unit.

Felson, M. 1995. Those who discourage crime. In J. E. Eck & D. Weisburd (Eds.), *Crime prevention studies*: Vol. 4. Crime and Place Monsey, NY: Criminal Justice Press, pp. 53–66.

Gallens, M. 2016. Pansy Tlakula appointed as new information regulator. [Online] http://www.news24.com/SouthAfrica/News/pansy-tlakula-appointed-as-new-information-regulator-20161026 (Accessed 20 June 2018)

Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q. and Laplante, P. 2011. Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political. *IEEE Technology and Society Magazine*, 30(1): 28-38.

Govender, I., Watson, BWW. And Amra, J. 2021. Global virus lockdown and cybercrime rate trends: a routine activity approach. In *Journal of Physics: Conference Series*, 1828 (1): 012107

Grant, C. and Osanloo, A. 2014. Understanding, selecting, and integrating a theoretical framework in dissertation research: Creating the blueprint for your 'House'. *Administrative Issues Journal: Connecting Education, Practice and Research*, 4(2):12-26.

Hamooya, C, Mulauzi, F, and Njobvu, B. 2011. Archival legislation and the management of public sector Records in Zambia: a critical review. *Journal of the South African Society of Archivists*, 44:116-123.

Han, C. and Dongre, R. 2014. Q&A. What Motivates Cyber-Attackers? *Technology Innovation Management Review*, 4(10).

Ioannidis, Y., Toli, E., Raheb, K.E. and Boile, M. 2014. Using ICT in cultural heritage, bless or mess? stakeholders' and practitioners' view through the eCultValue project. In *Euro-Mediterranean Conference,* Cham: Springer, pp. 811-818.

Jakimoski, K. 2016. Security techniques for data protection in cloud computing. *International Journal of Grid and Distributed Computing*, 9(1): 49-56

Kaiser, F., Wiens, M. and Schultmann, F. 2021. Motivation-based Attacker Modelling for Cyber Risk Management: A Quantitative Content Analysis and a Natural Experiment. *Journal of Information Security and Cybercrimes Research*, 4(2): 132-147.

Krubu, D.E. and Osawaru, K.E. 2011. The impact of information and communication technology (ICT) in Nigerian university libraries. *Library Philosophy and Practice*, (583): 1-19.

Lenaeus, J.D, O'Neil, L.R, Leitch, R.M, Glantz, C.S, Landine, G.P, Bryant, J.L, Lewis, J, Mathers, G. Rodger, R. and Johnson, C. 2015. *How to implement security controls for an information security program at CBRN facilities* (No. PNNL-25112). Pacific Northwest National Lab. (PNNL), Richland, WA (United States).

Li, X. 2017. A review of motivations of illegal cyber activities. *Kriminologija & Socijalna Integracija: Casopis za Kriminologiju, Penologiju i Poremećaje u Ponašanju*, 25(1):110-126.

Li, Y. and Liu, Q. 2021. A comprehensive review study of cyber-attacks and cyber security: emerging trends and recent developments. *Energy Reports*, 7(2): 8176-8186.

Liao, F. 2017. Analysis of Computer Network Security Problems and Countermeasures. In *2017 7th International Conference on Social Network, Communication and Education (SNCE 2017)* (pp. 905-908). Atlantis Press.

Masenya, T.M. and Ngulube, P. 2021. Digital preservation systems and technologies in South African academic libraries. *South African Journal of Information Management*, 23(1):1-11.

Masombuka, M, Grobler, M. and Duvenage, P. 2021. Cybersecurity and local government: imperative, challenges and priorities. In *ECCWS 2021 20th European Conference on Cyber Warfare and Security* (p. 285). Academic Conferences Inter Ltd.

McHugh, R. 2022. Different types of security in records management. [Online] https://www.recordnations.com/2019/01/different-types-security-in-records-management/ (Accessed 12 August 2022)

Netshakhuma, N.S. 2019. Analysis of the role and impact of the Mpumalanga provincial archives. *Mousaion: South African Journal of Information Studies,* 36(4):

Ngoepe, M., Mokoena, L. and Ngulube, P. 2010. Security, privacy and ethics in electronic records management in the South African public sector. *Esarbica Journal*, 29: 36-66.

Ngoma, M.L., Keevy, M. and Rama, P. 2021. Cyber-security awareness of South African state-mandated public sector organisations. *Southern African Journal of Accountability and Auditing Research*, 23(1): 53-64.

NI Cyber Security Centre.2020. Cybersecurity. [Online] https://www.nicybersecuritycentre.gov.uk/cyber-threats (Accessed 21 September 2022).

Nyampong, S.A. 2015. Electronic records management in national development: a case study in Ghana Immigration Service. *European Journal of Business and Management*, 7(10): 120-144.

Ocholla, D.N. and Le Roux, J. 2011. Conceptions and misconceptions of theoretical frameworks in library and information science research: a case study of selected theses and dissertations from eastern and southern African universities. *Mousaion*, *29*(2): 61-74.

Oyedum, G.U, Sanni, A.A. and Udoakang, I.O. 2014. Security and crime challenges in academic libraries in Nigeria. *Information Impact: Journal of Information and Knowledge Management*, 5(2): 127-140.

Prasad, S. 2022. Defending the public sector against increasing cybersecurity threats. [online] https://www.engineeringnews.co.za/article/defending-the-public-sector-against-increasing-cybersecurity-threats-2022-02-03/rep_id:4136 (Accessed 2 June 2021).

Ravitch, S.M. and Riggan, M. 2012. *Reason & rigor: How conceptual frameworks guide research*. Thousand Oaks, CA: SAGE.

Roos, A. 2016. Data protection law in South Africa. In A. B. Makulilo (Ed.), *African Data Privacy Laws,* Cham: Springer, pp. 189-227.

Salmons, J. 2019. *Find the theory in your research.* Thousand Oaks, California: SAGE Publications Inc.

Shafack, R.M. 2021. Securing Library and Information Resources: The Situation in Two State University Libraries in Cameroon. *European Journal of Education and Pedagogy*, 2(1): 25-31.

Sharma, R. and Purohit, M. 2018. Emerging Cyber Threats and the Challenges Associated with them. *International Research Journal of Engineering and Technology (IRJET)*, 5(2).

Sibhidla-Saphetha, N. 2013. The role of archives in fostering continuity in society. *Journal of the South African Society of Archivists*, 46: 74-80.

Silva, N.R. 2020. *Malware attacks on organisations*. Florida: Florida Institute of Technology.

Šimundic, S. Boban, M. and Šinković, Z. 2010. The regulatory and legal framework of information security and right to access information in Government, Local Government and Public Services. In *The 33rd International Convention MIPRO,* IEEE, pp. 1328-1332.

Sithole, T.G. 2019. Assessing resilience of public sector Information Systems against cyber threats and attacks: a South African perspective. PhD Thesis, Pretoria, University of Pretoria.

Toapanta, S.M.T, Cobeña, J.D.L. and Gallegos, L.E.M. 2020. Analysis of cyberattacks in public organizations in Latin America. *Advanced Science and Technology. Engineering Systems*, *5*(2):116-125.

Venson, S.L, Ngoepe, M. and Ngulube, P. 2014. The role of public archives in national development in selected countries in the East and Southern Africa Regional Branch of the International Council on Archives region. *Innovation: Journal of Appropriate Librarianship and Information Work in Southern Africa*, 48: 46-68.

Xu, M, David, J.M. and Kim, S.H. 2018**.** The fourth industrial revolution: opportunities and challenges. *International Journal of Financial Research* 9(2): 90-95. DOI: https://doi.org/10.5430/ijfr.v9n2p90

Yar, M. 2005. The novelty of 'cybercrime': an assessment in light of routine activity theory. *European Journal of Criminology*, 2: 407–27

Zazzau, V.E. 2007. *Transforming archives through information technologies: a bibliography*. Michigan: MI: M Publishing.

Zetter, K. 2018. 250,000 White House staffers, visitors affected by National Archives Data Breach. [online] https://www.wired.com/2010/01/national-archives-data-breach/ (Accessed 12 May 2021).