Journal of Theoretical and Applied Information Technology
15th January 2022. Vol.100. No 1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

CYBER-SECURITY KNOWLEDGE AND PRACTICE OF NURSES IN PRIVATE HOSPITALS IN NORTHERN DURBAN, KWAZULU-NATAL

IAN SINGH[1] , YASHIK SINGH[2]

[1]Author: Masters Student, School of Nursing and Public Health Science, College of Medicine – Tele-health, University of KwaZulu-Natal, Durban.
[2]Corresponding supervisor: Senior lecturer: School of Nursing and Public Health Science, College of Medicine – Tele-health, University of KwaZulu-Natal, Durban.
Email: [1]i.singh.sa@gmail.com, [2]singhy@ukzn.ac.za.

ABSTRACT

South African nurses work extensively with predominately paper-based medical information (patient/health records). Private secondary healthcare facilities are leading the transition towards digitised and interconnected Medical Information Systems (MIS). Electronic Health (eHealth) information is extremely lucrative on the black-market; therefore, large MIS databases (found in leading private hospitals) are prime targets for cybercrime. Employee negligence and human error account for almost half of database breach causes globally. Therefore, the security of MIS is significantly dependent on the MIS custodians (nursing, support, pharmaceutical, administration and management) utilising them. As South Africa transitions towards her eHealth strategic objectives, this study evaluated an essential element of information security – the cyber security awareness and practice of her MIS custodians. 185 MIS custodians working in two leading private hospitals in KwaZulu-Natal (KZN), were investigated and their reactions around cyber practice, cyber threats targeting end-users within the healthcare industry (viz. malware, social engineering, spam, phishing and Ransomware), and cyber awareness was evaluated. The results indicate a significant misunderstanding or ignorance of cyber and information terminology; lack of cyber security awareness and secure cyber practice; poor understanding of cyber threats and prescribed mitigations; and uncertainty pertaining to relevant legislation around electronic patient information. The current cyber security practice and knowledge of MIS custodians is concerning warranting intervention.
Keywords: *Cyber-crime; Tele-health; eHealth; Cyber-security; Medical Information Systems*

1. INTRODUCTION

Health information in South Africa (SA) is predominately still paper-based. Patient information is collected and stored in a traditional file with handwritten transcripts and the occasional X-ray or MRI scan. The Minority of electronic health information systems employed, have been fragmented, inconsistent and uncoordinated. They are typically heavily dependent on manual paper-based systems, are poorly automated and/or offer limited integration with other MIS systems [1]. Paper-based systems pose logistical challenges in terms of transfer, storage, backups, achieving and disposal of patient information. Healthcare facility filing rooms are quickly filled, resulting in historical patient information archived offsite; hindering analysis of patient trends, in support of their present treatment. Posting files from one location to another incurs inherent delays and increases the risk of data loss. Utilising facsimiles is promising, but creates duplicates, complicating the validity of current and accurate patient information. Maintaining the integrity and tracking access to paper-based patient files is challenging, because tradition filing rooms are restricted only by a locked door. Anybody with key could potentially gain unrestricted access to all patient files within the filing room. Furthermore, access to the filing rooms typically imply one could view, copy or amend any file in the room; thus, compromising data security, privacy, integrity, patient-safety and sound auditing principles. Paper-

based systems are a common cause of adverse incidents, because medical professional are unable to quickly discriminate and identify critical information amongst voluminous case notes [2]. In the modern medical working environments with high workloads, mistakes are common, passive paper-based systems cannot actively prevent potential errors or present/highlight important information like patient allergies.

According to the World Health Organisation (WHO), 44% of its affiliated countries report having fewer than 1 physician per 1000 people; furthermore the African Region suffers more than 24% of the global burden of disease, but has access to only 3% of health workers and less than 1% of the world's financial resources [3]. African medical professionals experience high workloads, further complicated by inefficiencies associated paper-based medical records. The lack of information inter-operability is prevalent in SA. Information Communication Technology (ICT) has the potential to revolutionise SA medical information management, through electronic data analytics, inter-operability, connectivity and mobility. WHO recommends the adoption of ICT into healthcare services to improve management, medical service delivery, efficiency and workload equalisation; known as electronic health (eHealth). Universal Health Coverage (UHC) is part of the "post-2015" agenda geared to meeting the Sustainable Development Goals (SDGs) adopted by the United Nations (UN) General Assembly in September 2015 [pg.5] [4]. The internet (commonly referred to as Cyberspace or Online) is the catalyst for globalisation, digitalisation, removing geographical boundaries, and creating a common platform for information-sharing and system-integration. Goal 3 is to "Ensure healthy lives and promote well-being for all at all ages" and its target 8 is to "achieve universal health coverage", to ensure that all people may have high-quality health services without suffering financial hardship" [pg. 5][4]. UHC cannot be achieved without the support of eHealth [Pg.5][4]. SA's healthcare is governed by the National Department of Health (DOH), which has committed to the adoption of eHealth [1].

South African nurses work extensively with predominately paper-based medical information (patient/health records). To effectively meet the increasing medical needs of the population paper-based medical record or filing systems must eventually become digitised and interconnected in the future. Private secondary healthcare facilities are leading the transition towards digitised and interconnected Medical Information Systems (MIS). Electronic Health (eHealth) information is extremely lucrative on the black-market; therefore, large MIS databases (found in most leading private hospitals) are prime targets for cybercrime. Employee negligence and human error account for almost half of database breach causes globally. Therefore, the security of MIS is significantly dependent on MIS custodians (nursing, support, pharmaceutical, administration and management) utilising them.

The study investigated the human elements, specifically the hospital MIS user (nurses, receptionists, support, pharmaceutical, administration and management), measuring self-perception, attitudes, awareness and abilities (behaviour and practice) of cyber-security issues. The objectives are exploratory and attempted to gain insight into the cyber-security practice and awareness amongst the medical information system users (MIS custodians). The study explored their knowledge, current practice and awareness around cyber security issues, investigating their understanding of cyber security terminology, pertinent legislation, best practice, risks and common cyber threat vectors viz. social engineering, spam, phishing and malware (viruses, ransomware, spyware etc.). The following research objectives underpinned this study:

- To assess the online usage of nurses;
- To determine the perceived awareness (knowledge) of nurses concerning cyber security issues;
- To determine the self-perceptions of nurses on cyber security issues;
- To determine the actual abilities of nurses in cyber security;
- To determine the attitudes and physical abilities of nurses on cyber security issues ; and
- To determine the motivation for current cyber security practice

1. LITERATURE REVIEW

As ICT integrates into healthcare, ICT vulnerabilities, risks and threats are also inherited. The DOH has recognised that with greater availability of information comes higher information security risks and has therefore stressed the protection of information security, confidentiality and patient privacy as key imperatives [pg. 9][1]. Information-security is a multifaceted process consisting of various aspects; cyber security is a subset of information security. Unfortunately, with the online digital revolution, crime has expanded into cyberspace, known as cybercrime. Crimes committed using the internet are more "convenient" (for the criminals), typically incur lower setup costs, pose a lower risk of apprehension and are therefore more profitable with a lower risk profile than traditional crimes [5]. Cybercrimes are typically committed using computer systems and do not necessarily require the cybercriminal to be physically present at the crime scene; therefore, it is difficult to catch cybercriminals. Local and international cybercriminal syndicates have a global reach, are well funded, difficult to track and due to jurisdictional challenges - even more difficulty to prosecute [6]. Cybercriminals are highly skilled and extremely intelligent. They target ignorant cyber users and seek to steal or ransom data, which offers them the greatest financial gain, on the black-market. Globally, during the last 8 years more than 7.1 billion identities have been exposed in data breaches [7]. In 2016, there were two separate waves of attacks involving destructive malware. Disk-wiping malware was used against targets in Ukraine in January and again in December, resulting in power outages [7]. Cybercriminal groups have grown in strength and are attacking large financial institutions, like the *Banswift* group attack in which US$81 million was stolen from the central bank of Bangladesh [7].

Cybercriminals find medical databases very attractive because, in addition to common information found on most databases, like identification numbers, physical address and credit card numbers, they also contain unique information, like next-of-kin, blood type, allergies, disease history and other highly sensitive information. Medical databases usually contain a high volume of records. The information within these records seldom changes or expires. Therefore, following a known data breach, some patient medical information (like allergies, blood type etc.) cannot be promptly changed to mitigate further loss (like credit card or mobile information). No wonder, medical databases are highly lucrative on the black market, fetching ten times more than a credit card number [8]. The healthcare industry is lagging behind other industries with regard to the protection of its infrastructure and health information systems (KPMG [9]. In addition, managers of healthcare facilities were found to have poor awareness of the sophistication of hackers and their means to infiltrate confidential patient data networks [9]. "The magnitude of the threat against healthcare information systems has grown exponentially" [9]. The mismanagement of health information and electronic health tools has far-reaching consequences for the public, industry and governments. Common types of exploitation and fraud include the sale of illegal medical credentials, human organ trafficking and blackmail. The illegal promotion and sale of medicines (including counterfeits, adulterated or unapproved drugs) and other products poses a risk to health and undermines legitimate trade. Healthcare security breaches and criminal attacks are rapidly increasing in frequency, scope and sophistication. Data breaches cause collective annual losses of $6.2 billion in the healthcare industry [10].

In 2015, three healthcare companies – *Anthem, Premera Blue Cross* and *CareFirst Blue Cross BlueShield* - were hacked. The *Anthem* breach was the largest – exposing some 79 million medical records. American legislation is comparatively more mature, better adopted and enforced, in terms of cyber-crime and management of electronic personal information and electronic medical information. The resultant personal liability lawsuits ultimately resulted in many of these medical companies going out of business. *Premera's* breach resulted in the exposure of 11 million medical records and *CareFirst*'s breach exposed over a million medical records [11]. In April 2017, the British National Health System was disabled by a Ransomware attack, resulting in the nationwide cancelation of scheduled procedures, massive delays and loss of functionality. Millions of patients were unable to receive medical attention. Hospital and medical centres across the country were unable to access

their medical healthcare systems. Microsoft advised that the attack was powered by a software tool developed by US national security association (NSA), which was stolen by hackers. This tool was used to gain excess to National health system (NHS) computers and install the Ransomware, which in turn encrypted electronic filing systems, thus crippling associated NHS systems. Microsoft released an update on March 14 that fixed this vulnerability, but Windows XP (used by some of the NHS computers) was unsupported by Microsoft since 2014, and computers that did not install the recent patch were left exposed. Failure to upgrade and update heath systems was the vulnerability exploited by the attack [12]. South Africa is listed globally, among the ten most vulnerable countries most susceptible to cyber-attacks [13]. Cybercrime in the South African context has shifted two places from sixth to fourth position, in terms of the economic crime index; with most respondents siting financial losses as the most damaging impact of a cyber-breach, followed closely by legal implications and reputational damage [14]. According to Dr Jabu Mtsweni, of the South African Council for Scientific and Industrial Research (CSIR), data breaches in South African are reported almost daily. Targeted attacks, denial of service (DDOS attacks), Phishing and Ransomware, are some of the cyber threats challenging South Africa. Many South Africa organisations, due to fear of reputational damage, fail to report attacks and breaches, thus creating a false sense of security and the incorrect perception that SA is not badly affected by cyber-attacks [15]. It has been reported that South Africa lost approximately R50 billion in 2014 due to cyber-incidents, and that over half a billion online personal records were lost or accessed illegally in South Africa during 2015 (SABC News, 2017). Estimates in 2011 put the financial losses from cyber-attacks at R3.7 billion in direct losses and R6.5 billion in indirect costs; furthermore criminal threats are forecasted to increase, as the number of South African Internet user's increases [16]. Most health information systems in South Africa are paper-based; therefore, as they become digitised and connected (online), cyber threats to medical information will also increase. In June 2020, one of Africa's leading medical healthcare service providers, Life Health, reported a cyber-attack on its southern African operation, which affected admissions systems, business processing systems and email servers, but is still determining the extent of data breached[17].

Human-user interaction within cyber space, remains a commonly exploited vulnerability [18]. A secure system utilised either ignorantly, insecurely, erroneously and/or without authorisation, creates a kink in the armour, thus compromising the security of the entire system, commonly resulting in a data breach. According to an IBM funded study, entitled *2016 Cost of Data Breaches* [10, 19] the healthcare industry had the highest per capita data breach cost in 2015. The average per capita cost of data breaches in South Africa in 2015 was $1.87 million. Threats to information-security along with cyber security are continuously developing and evolving; therefore, securing information systems, is an on-going cyclic process. The use of personal devices within the working environment and company devices/information outside of the company networks complicates security. Human error is an accepted natural occurrence. However, the scope of potential damage caused by human error over the last decade has changed dramatically. In the past, human errors like a healthcare professional losing a laptop or compromising a password may have only resulted in the exposure of a few hundred records; but today, with massive digitisation of medical information, system integration and online globally connected systems, the same error may expose millions of patient records. Employee negligence was identified as a top threat to information security - 36% of healthcare organizations and 55% of their business associates; named unintentional employee action as a data breach cause [10]. Globally, approximately fifty per cent (50%) of all 2016 healthcare data breaches were caused by criminal attacks, while the rest was caused by human error [18].

The review commenced widely by reviewing the global and local impact of cybercrime across all affected industries, which is devastating, rapidly increasing and cost is access of one trillion dollars , since 2018 [20]. Locally, cybercrime is among the top 4 crimes, as indicated on SA economic crime index; with financial losses as the most damaging impact of a cyber-breach, followed closely by legal implications and reputational damage [14]. SA cyber-attacks are increasing rapidly, because of developing ICT infrastructure and a population of

internet users which are inherently less aware of cyber threats, in comparison to first worlds populations [16] [5] [21]. Furthermore, SA is experiencing these threats in bulk for the first time (approximately 577 attempted attacks per hour), thus rudimentary cyber-scams are extremely successfully [21]. SA is listed globally among the ten most vulnerable countries most susceptible to cyber-attacks [13].

Narrowing the literature scope to cybercrime within the healthcare industry, there evidence of significant increase [10] and this industry previously and currently, consistently featured among the globally top targeted industries for cybercrime [22]. Increased security risks in healthcare can be attributed to a high demand for electronic medical records on the "Black Market", the high acceptance and tendency for doctors, nurses and other staff to bring their own devices (smartphones, tablets and laptops) to work, and a long history of limited investment in health information security [23]. Globally, many healthcare companies have been bankrupted, shortly after cyber breaches [11], but no comparable similarities were found within the SA healthcare industry. However in June 2020, one of Africa's leading healthcare service providers (Life Health) experienced a cyber-attack on its Southern African operation, the extent of the data breach was undetermined and under investigation [17]. SA legislation around medical information and the reporting of data loss/breach has not yet been fully established within legislation, this may account for the comparatively low reports of data loss/breach within SA healthcare. Furthermore, because SA is still developing towards a fully electronic and interconnected health system [24], this may also account for the relatively reported incidence of cyber-attack within SA healthcare. In response to the increase in global cyber-attacks within the healthcare industry, a multidisciplinary team of experts been banded to analyse threats, promote interdisciplinary discussion, and to propose practical recommendations for hospitals across the globe; recommendations which have defined the structure of this studies recommendations [25].

Within the literature there is strong theme around the exploitation of computer users in most cyber-attacks [26]. Globally, analysis of cybercrime related emails(SPAM) found healthcare workers were among the most targeted of employees [26] and the most effective method for compromising hospital MIS and networks, was phishing attacks (typically sent via email) which exploit human weakness in decision-making through tactics such as asserting authority, time pressure and urgency [27]. Furthermore, the literature indicated that approximately one out of every two healthcare breaches was caused by human error or ignorance [18]. The common types of cyber-attacks targeting computer users within the health industry correlate with those included within the scope of this study, viz. social engineering, spam(unwanted email), phishing and malware (viruses, ransomware, spyware etc.).

A scoping literature review of four databases (*PubMed, Web of Science, ProQuest*, and *Scopus*) for relevant manuscripts related to cyber-attacks against hospitals and available best practice, published between 1997 and 2017; identified six domains of research: context and trends in cyber-security (27.8%), connected medical devices and equipment (29.9%), hospital information systems (14.4%), raising awareness and lessons learned (6.2%), information security methodology (15.4%), and specific types of attacks (6.2%) [28]. The study concluded that there is a growing interest in the research field; the literature remains limited in number and certain aspects of cyber-security have been neglected; and comprehensive guidelines and standards are lacking [28]. This concurs with the search review conducted on PubMed, with little research focused specifically on the cyber practice and knowledge of end-users working within the health industry of a developing country.
Review of within the African healthcare industry found partial similarities -:

A Nigerian study showed target population and socioeconomic similarities, demonstrating the unique challenges of developing countries were comparatively little or late exposure to ICT, affects the adoption, knowledge and skill of ICT. However, is differs in scope as it was focused on basic computer operation. The assessment of the knowledge and utilization pattern of information technology among health care professionals and medical students in a university teaching hospital in Nigeria, found that only 26% of the respondents possess a computer, only a small percentage of

demonstrated good knowledge of computers and IT, and showed suboptimal utilization pattern of ICT. Furthermore, health records officers, who by virtue of their profession had better training opportunities, also did not indicate significantly better knowledge and utilization habits [29]. The study recommended the need for a more structured ICT training curriculum for nurses, rather than ad hoc training [29], which concurs with the training recommendation of this study.

A similar study of computer skills of nurses in Lesotho, found that about 61% of their nurses had inadequate skills in computers, because of developing world challenges like year of obtaining latest qualification, sex(being female), and computer experience (lack of exposure to computers at school or during nursing training) [30]. The lack of basic computer competency in comparison to developed nations were most nurses were introduced to computers in primary school and had ample exposure to ICT prior to commencing their nursing training is a significant factor that must be considered when adopting MIS into the healthcare systems of a developing nation. The study indorsed the challenges of developing nations be considered during planning of a training curriculum for nurses and recommended in-service training in computer skills for Lesotho nurses to improve the implementation of MIS and general healthcare delivery [30].

Partial similarities were found with a South African, Kwa-Zulu Natal study [31] which was focused on existing legislation (at the time which has changed), data backup, and storage and encryption practices. The study aimed to determine the use of computers by healthcare practitioners in the workplace and home which included the use and approach to data storage, encryption and security of patient data and patient email and the use of informed consent to transmit data by email. There are sample target similarities except the study was not focused on secondary healthcare facilities. There are partial contextual scope similarities however; this study has focused on cyber-security practice of private hospital staff and only basic knowledge terminology regarding encryption and current relevant legislation around electronic medical information.

The study has some methodological and theoretical similarities to a recent study in which the cyber-security awareness of students was investigated [32] and found student lacked the knowledge and skills or behaviour around best practices in cyber-security awareness. However, there are obvious target population differences, as this study was focused on the cyber practice and knowledge of MIS custodians within the private secondary health industry. Comparatively, developing countries like SA have unique population challenges with regards ICT. South Africans are generally under-skilled in ICT in comparison to countries like the US. EHealth transformation creates the opportunity for cyber threats to compromise the safety of MIS, by exploiting a potential human vulnerability. South African companies have the highest percentage of data breaches attributed to human error; and both South Africa and Brazil have the highest estimated probability for data breach occurrence [19]. Acknowledgement to the many unmentioned studies touching on similar areas; however, the issue described is critical, warranting dedicated attention. Uncovered study similarities were discussed, but overall, this study is believed to be unique in its scope and focus on addressing a gap in the literature were more research is required. Considering current SA cybercriminal trends and highlighted themes, it is imperative that the current cyber practice and knowledge of MIS custodians are assured, prior to increasing cyber exposure of SA MIS through planned integration.

2. METHODOLOGY

The requirements for ICT in healthcare have been established by numerous studies. The global initiative championed by WHO is underway in South Africa. Most public hospitals in South Africa are using traditional paper-based information systems. South African public health systems are struggling to meet the increasing public healthcare demand. Most public healthcare facilities are poorly maintained, underfunded, understaffed, inadequately equipment, inefficient and/or over capacitated. South Africa is currently engaged in the complex task of reforming the public health through collaboration, cooperation and integration with the private healthcare sector, through the formation of a National Health Insurance (NHI) system. South

Africa does not have an integrated public MIS; however, a few private healthcare groups have initiated independent MIS. These do not readily integrate with systems outside their group. Currently, private healthcare facilities lead healthcare provision, quality and technical innovation. Upon implementation of the NHI, successfully employed processes, systems and innovative technologies currently employed within private healthcare, may be adopted or influence the development of common systems and processes (like MIS). Hence private healthcare groups were targeted. A random sample of hospital support staff (nurses, receptionists, support, pharmaceutical, administration and management) with access to MIS, was evaluated.

At the time of investigation, two predominate private secondary healthcare groups were found to be leading the transition toward electronic patient healthcare systems. The first was still very much in its infancy, heavily reliant on traditional paper-based systems, fragmented and mainly limited to patient billing information systems. The second group was found to have a more developed and integrated MIS and limited electronic patient data integration (between nursing, support, pharmaceutical, administration and management). Two hospitals from the second healthcare group within northern Kwa-Zulu Natal were targeted, as research sites. Target sites were evaluated based on the hospital's utilisation of MIS and proximity to the locality of the researcher (as the study was self-funded).

South African doctors have extremely high workloads, therefore the updating of patient electronic health records are typically delegated to hospital support staff (nurses, receptionists, support, pharmaceutical, administration etc.) and was identified as the target population The studied aimed to evaluate the cyber awareness and practice of these workers, hence is was imperative that the hospital support staff evaluated owned online capable devices like laptops, smart phones, tablets and personal computers) and engaged regularly in internet/online activity. The hospital support personnel which were evaluated represented all race groups in South Africa and are classified in the higher *Living Standards Measure* (LSM) categories. As the targeted population, earned more than their colleagues working in public hospitals and other areas, it was more plausible that they with meet the criteria. Surveyed results confirmed the validity of primary assumptions viz. all participants owned online capable device/s and regularly accessed the Internet via private and/or public LAN's, cellular and/or Wi-Fi; both within and outside of the hospital environment.

Data was collected via a questionnaire and analysed using MS Excel and Google analytics. The questionnaire was initially reviewed by peers and nurses, to remove errors, ambiguity and misunderstanding. Targeted sites were short-staffed with high workloads and long non-office working hours (shifts). The sensitive hospital environment, restricted access and shift rotation; made conducting fieldwork at the chosen sites, extremely challenging. Site management was understandably protective and offered limited assistance towards the facilitation of survey administration. Hospital group email distribution was unsupported and groups IT policies denied access to hospital network and online forms. The research was allowed access to designated areas only. Therefore, the researcher facilitated electronic online surveys by providing both devices and personal internet access to the target population. However, due to high workloads, shift rotation and restricted access to hospital wards, a mixed method of distribution was utilised, consisting of researcher facilitated group electronic surveys and non-facilitated paper surveys. Target numbers were evaluated based on complexities and challenges mentioned from the selected sites. Target sample numbers were calculated using an online calculator [33]. Prior to the commencement of fieldwork, the identified target population was 352. Data from 184 usable inputs was extrapolated and analysed from multiple visits to two sites, over a period of two months. Calculations, using an online calculator (Systems, 2012), indicate that a targeted confidence interval (margin of error) of 5% with a confidence level of 95%, was be achieved.

The study utilised the Theory of planned behaviour (TPB) to understand the cyber awareness and practice of hospital MIS users[34]. TPB has been used in investigating an individual's ethical behaviour and decision to adopt acceptable computer security measures and comply with these measures (Lee & Kozar, 2005; Leonard, Cronan, & Kreie, 2004; [35]. The study was exploratory, focusing on the medical information system user (nurses,

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

receptionists, support, pharmaceutical, administration and management), measuring self-perception, attitudes, awareness and abilities (behaviour and practice) of cyber-security issues. The objectives are exploratory and attempted to gain insight into the cyber- security practice and awareness amongst the medical information systems user (nurses). The study explored their knowledge, current practice and awareness around cyber security issues. A quantitative approach was utilised to assess the independent variable (i.e. cyber-security self-perception, attitude and ability), and the dependent variable cyber-security awareness.

In this study data was collected about the nurse's attitudes, beliefs and practice in the domain of cyber-security awareness. These attitudes, beliefs and practice do not naturally exist in a quantitative form, therefore to facilitate the collection of quantitative data, a questionnaire using both closed-type questions and Likert Scale type questions, was employed. Furthermore, these exist both within and outside of their working environment (hospitals), hence the study tested both private and professional environments. Data was correlated to determine whether cyber-security awareness and practice was safe or if further mitigation, perhaps in the form of training to improve cyber-security practice amongst nurses, is required.

The research design employed was similar to a recent study which investigated the cyber-security awareness of tertiary students [32], but this study specifically targets healthcare professionals utilising medical information systems, focusing on the prevalent cyber-security risk to hospitals. The study found that tertiary students lacked the knowledge and skills or behaviour around best practices in cyber-security awareness, and recommended intervention in the form of cyber-security awareness training. This study also has some similarities to a study by [31] which was focused on existing legislation (at the time which has changed), data backup, storage and encryption practices. The study aimed to determine the use of computers by healthcare practitioners in the workplace and home which included their use and approach to data storage, encryption and security of patient data and patient email and the use of informed consent to transmit data by email. There are sample target similarities; however, the scope of this study was focused purely on cyber-security.

The study scope excluded the following: group IT policy, IT network configuration, hardware configuration, software and application configuration and/or technical standards and maintenance methodology employed by the evaluated hospitals. The study did not evaluate the compliance or enforcement of legislation; instead it explored the current knowledge of pertinent legislation, amongst the target population. The study investigated the online activities of healthcare professionals (utilising MIS) – within and outside the hospital environment. The intended inter-utilisation of personal devices and hospital devices between personal and hospital network, was explored. The knowledge of cyber-security terminology, basic cyber threats and attacks, current attacks, unsafe and safe cyber practice and the knowledge of pertinent legislative acts; was explored. The reaction of nurses to symptoms of cyber threats, targeting end-users within the healthcare industry (viz. malware, social engineering, spam, phishing and Ransomware), was evaluated. Online activities were evaluated to describe potential risk of exposure to cyber threats. The cyber security practice and maintenance of personal devices (viz. antivirus, software updating/ patching), was evaluated to establish vulnerability to cyber-threats. Intent to transfer data between personal and hospital devices and/or networks, was be evaluated.

Legislation in South Africa, relative to cybercrime was not definitive, until recently with advent of the Cybercrimes and Cyber-security Bill (CAC). The *South African Constitution* entitles all South Africans to the right to privacy. "The Constitution guarantees citizens the right to privacy, including the right not to have the privacy of their communications infringed (Society, 2014:12). In terms of Section 74 of the National Health Act, the National Department of Health (NDoH) is responsible for the facilitation and coordination of health information, hence responsible for the eHealth policy and strategy development. It is unlawful to divulge an individual's health information, without his/her consent. The only permissible exceptions are when the law or a court order requires disclosure, if non-disclosure would represent a serious threat to public health, or if disclosure may assist in the prevention or detection

of a crime that will put someone at risk of death or serious harm [2] (p12).

The Protection of Personal Information Act of 2013 (POPI), governs how organisations use, process and manage personal information and how this information is protected [36]. This Act implies that all employees are legally obliged to treat all personal information concerning all patients, including their health information, as private and confidential. *The Electronic Communications and Transactions* (ECT) Act 25 of 2002 impacts on electronic communications and transactions and applies to any form of communication including (amongst others) e-mail, the internet, SMS; except for possibly voice communications between 2 people. However, according to a 2013 study entitled *Pitfalls in computer housekeeping by doctors and nurses in KwaZulu-Natal: no malicious intent* [31] it was concluded that most healthcare professionals, as sampled in South Africa, are not compliant with the National Health Act or the ECT Act of South Africa. The CAC could possibly aid the reporting of cybercrime and encourage South African companies to invest more in
information security, because it is more prescriptive and emanates from the lack of businesses not reporting data breaches and the loss of personal records/information.

3. RESULTS AND DISCUSSION

3.1 Self-perception or belief of MIS Custodians

Most participants believed they were competent online (63%) and are concerned about online security (60.9%). Positively, most (69%) are concerned about the safety of MIS; and the majority (88%) believe they are legally responsible for the medical information they work with. Unfortunately, this was tainted by poor knowledge and lack of understanding of the corresponding law (expanded in the following subsection).

A little more than half (52.4%) have attended cyber security/internet/online training and the majority (95.7%) of them rate their online/cyber skill as competent or above. This is reasonable, as almost all (whom have attended training) are probably confident in their cyber ability, because they are more experienced and familiar with internet/cyber terminology and associated aspects.

Table 4.1.1: Cyber training and Self-rated Skill Level

	Attended cyber security / internet security/ online security training				
Self-rating of internet/online skill level	**Yes, at work/ hospital**	**Yes, at college / varsity university**	**Yes, at school**	**No, never**	**Skill level Total**
Novice (beginner)	4	0	0	24	28
Competent	52	6	6	52	116
Advanced	20	3	4	12	39
Expert	0	0	2	0	2
Total	**76**	**9**	**12**	**88**	**185**

Of the 47.2% that have never received training, only 27.2% rate their skills as beginners/novice. It is reasonable, that most of the self-rated novices/beginners have never received training, because they are probably less familiar with internet/cyber security terminology and associated aspects. 95.8% of those that have received training believe their internet/cyber skills are competent or better, however, it is unusual that 72.3% of those, whom have never had training, regard their online skills as competent of better. It is likely, that some may have an overrated self-interpretation of their cyber skills. This can be dangerous as there are more likely to assume high level cyber task and less likely to execute them safely.

Unpatched operating systems and failure to update security software regularly; are commonly exploited by hackers and increase device susceptible to contracting malware online [7]. Unfortunately, only about half of MIS custodians believe their personal devices require regular operating and security software updates. Ransomware, Phishing, Social engineering and various other Malware based threats, are typically initiated via email; 1 in 131 emails, were found to contain malware (highest rate in five years) [7]. These malicious emails are disguised as routine correspondence (such as invoices, delivery notifications or general correspondence), from familiar mail recipients (such as banks, friends, colleagues, government department etc.). Almost half (44.6 %) believe that their friends would not send them emails containing malware. Therefore, 44.6% are likely to open an unsafe email. 60.9% of participants are very concerned about security on the internet; 60.9% are very concerned about banking on the internet; and 42.4% are very concerned about downloading online content. Most participants (62%) are very concerned

about the safety of the information they work with in the hospital, while the minority (7.6%) are not concerned. Majority of participants (88%) believe they are legally responsible for the information they work with, while 16.4% are unsure and 13% believe they are not legally responsible. Although, the concern and sense of legal responsibility is commendable, the severe lack of knowledge of safe cyber practice and pertinent legislation in concerning.

Approximately 42% of participants believe their personal devices are protected from malware, while approximately 63% believe that their work devices are protected from malware. 26.9% of participants believe that updating of security software and operating system software, on personal devices is annoying, time consuming and uses up too much data (from pre-paid data bundles), while a further 23.9% are unsure. 12% of participants never update their device software, 26% rarely update and only 28.3 % update it monthly. Unpatched operating systems and failure to update security software regularly; are commonly exploited by hackers and increase device susceptible to contracting viruses online [7].

Approximately, 16% believe it is fine to use their personal devices on the hospital network, while approximately the same are unsure. Approximately 7% believe it is fine to use hospital devices on their personal network while about 5% are unsure. 86.9 % believed that their personal devices should not be used to access patient records, while 6.5% were unsure and 7.6 believed that it was fine to access patient records from their personal devices. Similarly, the majority (83.6%) believe it is not fine to access patient records via personal or private networks, while 8.7% are unsure and 8.6% believe in is fine. Although of the minority, the intention to utilise personal devices and hospital devices interchangeably between private and hospital infrastructure, is evident.

The majority (66.3%) believe that the information systems they work with are secure, while 21.7% are unsure and 12% believe that they are insecure. Only, 23.9% are confident with their current level of internet security and cyber security awareness, while 47.8% are unsure and 28.3% are not confident. Of concern, is a significant 32%, believing it is safe to utilise personal devices on hospital networks and a further 12% that believe it is safe to utilise hospital devices on personal networks. Slightly more than half (54%) of participants are confident that their cyber security practice (themselves and their colleagues) within the hospital environment, is safe. Generally, there is significant evidence of cyber security misunderstanding, uncertainty about information security issues and lack of confidence in both individual and collective safe cyber security practice. 72.3% of those, whom have never had training, regard their online skills as competent of better. Overrated belief in online/cyber skill is dangerous, because of the tendency of these users (self-rate advanced) to engage in cyber or online activities (that demand a solid understanding of higher online information systems) were incorrect/poor cyber practice may have deeper and far reaching consequences. Furthermore, self-rated advanced users may be more susceptible to social engineering threats, as because of their ignorance they are typically less cautious and less likely to seek assistance.

3.2 MIS Custodians Knowledge of Cyber Security Matters

The knowledge of pertinent South African legislative acts governing the handling of medical and electronic information was tested. Results are as indicated in the figure (below).

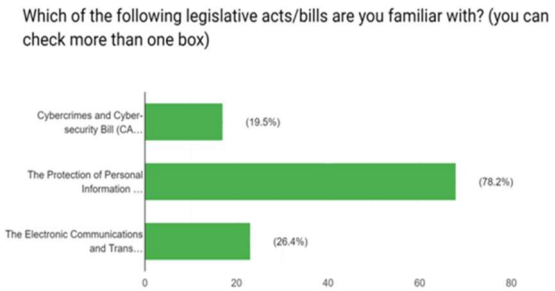

Figure 4.2.1: Knowledge of South African Legislative Acts, Pertaining to Electronic Medical Information

Only the minority were familiar with the recently passed Cybercrimes and Cyber-security Bill (19.5%) and the Electronic Communications (26.4%) and Transactions Act. The Cyber Security Bill describes the responsibility for public data, reporting procedures for data-breach/data-loss and implications of data-breach/data-loss. Only 62% of participants (62%) correctly understood what a Data-breach was. Poor awareness of basic terminology

and common threats contradict with their self-perceived online competency. Although 78.2% were familiar with the Protection of Personnel information Act (POPI), I suspect most are not fully aware of its practical implications, because it has not been fully implemented. Once, fully implemented it will enable citizens, as data subjects, to bring civil actions against firms for data breaches. It will therefore require all companies holding personal information, to bolster their cyber security efforts, with additional staff and significant cyber security personnel deployment and development, from grassroots up to board level. The Electronic Communications and Transactions (ECT) Act of 2002 sets out principles for information protection and created offences of unauthorised access to, interception of and interference with data. However, it appears to have had little practical effect[37]. These acts all impact the protection of patient information. Sound knowledge and understanding of all these acts are required to effectively protect electronic patient information. Although the majority claim to comply with the current legislation, given the general lack of knowledge of all three acts; it is probable that the actual legislative compliance among participants is lower than their perceived compliance.

4.3 Cyber Security Knowledge of Nurses

The study evaluated theoretical knowledge of MIS custodian, by testing the definition of basic cyber security terminology, concepts, symptoms of cyber threats - targeted at end-users within the healthcare industry (viz. malware, social engineering, spam, phishing and Ransomware). Less than half, correctly understood basic terminology about cyber related issues (strong passwords, Antivirus, information passed as part of a typical web page request, Ransomware and Phishing). The majority understood the purpose of encryption (79.3%). More than half of participants (67.4%) understood what Spam was, but less than half (42.4%) understood all the characteristics of strong passwords. Only 37% understood the purpose of Anti-virus software and less than 10% of the participants understood all the information their devices potentially share online, as part of a simple webpage request. According to a literature review of Ransomware attacks on health information systems, Ransomware is among the leading cyber security threat harbingering the medical industry[38]. Only 21.7% knew what Ransomware was; and less than half of participants understood what Phishing was (45.7%). Only 62% of participants correctly understood what a Data-breach was. It was evident that knowledge about basic cyber security is lacking, with misunderstanding among the majority.

Table 4.3.1 – Analysis of Correct Theoretical Knowledge and Self-rated Skills

	Self-rated Internet/ Cyber Skills					
Correct theoretical understanding of following cyber terminology	Novice (% correctly answered)	Competent (% correctly answered)	Advanced (% correctly answered)	Expert (% correctly answered)	Total - correctly answered	%
Phishing (Unsolicited requests (usually sent via email) to fool receivers in divulging personal information)	2 (7,1)	52 (44.8)	28 (71,7)	2 (100)	84	45.4
Antivirus (to protect your computer /devices against malicious software)	6 (21.4)	40 (34.5)	21 (53.8)	2 (100)	69	37.3
SPAM (Unwanted email that usually contains malware)	10 (35.7)	80 (69)	33 (84.6)	2 (100)	125	67.6
Encryption (prevent unauthorized access to information)	18 (64.3)	92 (79.3)	37 (94.9)	0 (0)	147	79.5
Data breach (Unauthorized access to files and/or information)	10 (35.7)	72 (62.1)	31 (79.5)	2 (100)	115	62.2
Ransomware (an attack which encrypts the files of the infected system)	0 (0)	24 (20.7)	14 (35.9)	2 (100)	40	21.6
Total (according to self-rating)	28	116	39	2		

Table 4.3.1 shows all self-rated experts have the correct theoretical understanding of all listed terminology, except for encryption. Self-rated notices, theoretical understanding was consistent with their self-rating; unexpectedly some novices understood encryption, while nil experts understood the term. Most self-rated competent MIS custodians misunderstood Ransomware, antivirus and phishing terminologies; however most understood data breach, spam, encryption terminologies. Accept for Ransomware, which is a relatively new threat vector, competently skilled users should have an accurate understanding the remaining terminology, hence it is evident that online/cyber skills of self-rated competent MIS custodians, are overrated. Similarly, most self-rated Advanced MIS custodians understood spam, encryption and data breach terminology, but most misunderstood phishing and Ransomware terminology. Advanced users are expected to have a sound understand of these basic concepts; hence their self-rated skills are severely overrated.

Generally, the study found that participants self-evaluated online/internet knowledge was overrated. Alarmingly, less than half, correctly understood basic terminology, concepts and threats about cyber related issues; thus indicating an above average risk (i.e. more than the global industry probability of 50%) of human error (unintentional or unknowingly) contributed data breaches [18]. Furthermore, the general lack of familiarity with current legislation governing information security, protection of

information, electronic communication and cyber security; pose a significant legislative and financial risk, supporting intervention, perhaps is the form of a training program, comprising of foundation modules and annual refresher modules (see conclusion).

3.4 Online Abilities or Skill of Nurses

Most participants (more than 80%) use online services daily, for instant messaging, private email, web-browsing, uploading/downloading and social media. On average, social media and instant messaging are the most popular online activities; with participants spending more than two hours (average per a day) engaged in these activities. The utilisation of *WhatsApp* (mobile social networking application) among healthcare professionals to communicate patient information is increasing, because it was a simple, cheap and effective means of communication. However confidentiality, consent and data security were often overlooked; and required further guidelines for general utilisation, legal compliance, device (personal and hospital) utilisation and data transfer (encryption) of health information [39]. According to the CSIR, South Africans share too much of their personal information on social media, allowing cybercriminals to exploit them for their personal gain [40].

Table 4.4.1: Analysis of MIS Custodians that Belief their Cyber Practice is Safe (within the Hospital Environment), in Comparison to their Personal Cyber Practice

	UNSAFE			SAFE		53%
Safe Cyber Security Practices -:	Strongly Disagree	Disagree	Unsure	Agree	Strongly Agree	In a professional capacity, the cyber security practice of my colleagues and I, are safe (i.e. we always ensure work data is secure)
I download files from only reputable sites	18	8	22	20	32	100/185
I regularly check my privacy settings on my browser and social networks	20	16	30	6	28	100/185
I change my passwords regularly, at least once a month	12	8	16	8	56	100/185
I keep myself updated with the latest internet security threats reported in the media	12	22	26	22	18	100/185
I don't open email attachments or links if it looks suspicious.	4	6	14	16	60	100/185
I am careful about the websites I visit, checking protocol, like "https "and correctness of the URL (the website name on the address bar)	0	8	24	22	46	100/185
I turn on updates for all my personal devices (like windows, mac and android) and install security plugins and add-ons for my web browser	8	16	22	28	26	100/185

In their professional capacity, only 53% are confident (agree or strongly agree) that their personal cyber security practice and that of their colleagues, are safe (i.e. they always ensure work data is secure). Analysis (Table A1) reveals that of the 53%, only 66% would definitely not open suspicious emails; only 68% are always careful about the website they visit; only 40% are aware of the latest internet security threats reported in the media; only 64% change their passwords monthly, only 34% regularly check their privacy settings on browsers and social networking application; and only 52% download files exclusively from reputable websites.

In addition, of the 53% whom are confident (agree or strongly agree) that the cyber security practice themselves and their colleagues, are safe; only 54% update all their personal devices (like windows, mac and android) and install security plugins and add-ons for my web browser. Good cyber practice is habitual; hence poor personal cyber practice is could continue hospital devices and networks. Appreciatively, on most hospital networks, dedicated IT professional are typically responsible for ensuring all hospital devices are regularly updated and software vulnerabilities are plugged. However, users that are cognisant of out-dated software, because of good personal cyber practice increase cyber-awareness and reduce the risk of cyber breach. Moreover, 16.3%% believe it is fine to use personal devices on hospital networks and a further 17.4% are unsure. 7.6% believe it is fine to utilise hospital devices on personal networks, hence the probability of cross-contamination between hospital and private devices and networks, is evident, making the personal cyber practice of hospital staff more relevant, as poor cyber practice and unpatched or outdated software, introduces vulnerability to both personal and hospital networks, devices and data. 54.3% of MIS custodians believe that the cyber practice of themselves and their colleagues, within their professional environment, is safe. However, many may not know the difference between safe and unsafe cyber practice. Disregard for basic safe cyber practices is evident; and ignorance of basic terminology, common cyber threats and legislation, is prevalent. Hence the safe cyber practice of participants within sample population is significantly lower than then then 54.3%.

Approximately 66% use online banking and streaming. 33% of participants don't engage in online shopping or gaming. Approximately 15%

indicated that they use torrent services. Torrent services typically pose higher security risks [41]. Torrent services are peer-to-peer services, meaning bits of data are shared between all connected users, thus significantly increasing the probability of contracting viruses. Most company firewalls are configured to block access to torrent websites. If the hospital network is configured block access to torrent websites, there is residual risk of system infection from infected private/personal devices, which access the hospital network.

Majority of participants utilised mobile networks (46.7%) to engage in internet/online activities, while 16% used private home networks. Almost 35%, accessed internet and online facilities from work, which is perhaps a major area of concern, depending on the network security infrastructure, policies and configuration. Healthcare companies are under increases pressure from physicians, nurses, and other medical staff to support personal devices access (like tablets, smartphones, and laptops)on healthcare networks (databases) Finding a balance between allowing access of personal device (BOYD) and maintain information security, is challenging, fundamentally, because these devices are not owned by the healthcare company and therefore are not necessarily subject to their configuration, policies and restrictions. A recent study published in the BMC Medicine Journal revealed that 66% of health software applications sending identifying information over the Internet, do not utilise encryption, while 20% do not have a privacy policy [42]. Less than half (43.5%) of participants updated personal devices operating systems, security plugins and add-ons on their web browser/s, while 25% are unsure and approximately 31.5 % do not. Unpatched operating systems, outdated security software (anti-virus) and outdated web browsers are commonly exploited vulnerabilities which can be easily addressed on hospital devices, but not on personal devices. Results indicate that 56.5% of participant's personal devices are vulnerable to cyber-attack. Securing personal devices, to ensure they are free from malware and safe to access the hospital network is a difficult challenge.

Only 29.4% of participants keep themselves updated with the latest internet security threats reported in the media, while 31.5% are unsure and 39.1% do not. Cyber security threats are consistently evolving, becoming ever more sophisticated and difficult to detect. Cyber security awareness groups are a key mitigating because by it developing user awareness. Users are less likely to become victims, once alerted and adequately educated about an of an attack occurrence (breach). A critical part of a healthy security system is the provision of regular security threat information to end-users. Increased effort toward the development of awareness of cyber security threats and related issues would be beneficial.

Refreshingly, most participants (76.1%) do not open suspicious emails, however 12% indicated that they might and 11.9% indicated they would, open suspicious emails. Spam is the leading distribution mechanism for most malware and social engineering threats and often forms part of large more destructive cyber-attacks. Hence, the potential risk posed by 23.9% of participants a concern, especially if devices are shared between private and hospital networks. Positively, most participants (87%) are not comfortable sharing passwords with co-works or seemingly trustworthy people, while 5.4% are unsure and 7.6 are comfortable sharing their passwords. Although only the minority are comfortable sharing passwords, it is a commonly exploited vulnerability utilised in social engineering attacks (like Pretexting); to access unauthorised access to medical database. Coincidently, only 59.75% change their passwords regularly (once every month) and only 25% regularly check their privacy settings their browser and social networking applications. Unchanged and the use of the same passwords on multiple applications or devices, maybe vulnerable to brute force attacks (an algorithm uses know information to calculate all probable passwords, often succeeding by process of elimination).

20.7% of participants elected to disable security settings and tools that they felt were pesky or slowed them down, while a further 26.1% may possibly disable them. System security tools and setting are designed to protect users from certain types of attacks, having the most updated operating systems and anti-virus software updates are useless, unless they are enabled. On hospital networks changes to these security settings typically require system administrator level authorisation, however, mere the fact that 48.8% may intent to disable these settings,

is an important indication of ignorance and/or unawareness of cyber security good practice and cyber threats.

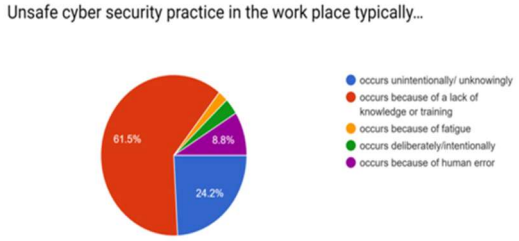

Figure 4.4.1 Causes of Unsafe Cyber Security Practice in Hospitals

The majority (61.5%), believe that possible unsafe cyber security practice, may be attributed to a lack of knowledge or lack of training, while a further 24.2%, believe it occurs unintentionally. Most participants have not received any form of formal of online/internet or cyber security training (47.8%), which is concurs with finding by the CSIR stating there is a strong requirement to increase the level of security awareness of various technology users and ICT security practitioners[43] . The majority of those, whom have received training, have received it at work/hospital (41.3%), which is positive reflection of the company's attitude to online/internet/cyber security training; however, the scope and frequency of training is unknown. Due to rapidly evolving cyber threats and information systems, once-off training may quickly become out-dated, ineffective and/or irrelevant. On completion of the fieldwork, more than half of those surveyed, had not yet received training.

Only 57.6% of participants are cautious when visiting websites, checking for "https" protocol and the correctness of the URL (the website name on the address bar), while 29.3% are unsure and 13.1% are not cautious. Although most participants are cautious about online security protocol, a significant amount are simply unaware or unsure; thus, making them susceptible to phishing and associated cyber threats. The cyber security practice of participants is concerning, especially on personal devices. The study showed that 56.5% of participant's personal devices are potentially vulnerable to cyber-attack. The majority engage in online activities including social media, online shopping, gaming and streaming. Alarmingly 15% access torrent websites and there is a significant lack of appreciation for cyber security tools and protocols. Furthermore, the majority are unaware of the latest cyber security threats, thus making them susceptible to cyber-attack. Essentially, we have a fair amount of poor cyber savvy MIS Custodians, engaging in online activities that attract higher cyber treat attention. Assuming, the interchangeable utilisation of personal and hospital devices between personal and hospital networks is prevalent; the current cyber-related practice of participants may pose major security risks to hospital infrastructure and patient data.

3.5 Assessment of Scenario-based Responses

Scenario-based questions are commonly utilised to test an individual's re-action, based on their understanding, knowledge, skill and belief around a specific event or topic. Therefore, a scenario approach was utilised to explore the reaction of MIS custodians, towards commonly employed cyber threat vectors which attempt to breach personal and private system security.

4.5.1.1 Breached personal device scenario

In the first scenario, figure 4.5.1.1 (below), participants were posed with evidence, suggesting a hack/breach in progress, of a personnel device. Only 43.5% correctly selected to disconnect the device form the network (the best course of action, because it would disconnect a hacker and give the user opportunity to salvage any unsaved data). 30.4 % choose to switch off their device (which will terminate the hack, but risk possible data loss, software damage and/or hardware damage. Interestingly, 7.6 % choose to disconnect the mouse, while 9.85 choose to leave the device and call someone to observe the occurrence; both actions allow the hack to continue to spread through the device, network and other connect devices. Alarmingly, 8.7% elected to connect the device onto the hospital network (so that hospital IT could attempt to fix it) thus giving the hack access to hospital devices and data. Again, these actions although seemingly harmless, could easily directly threaten the hospital network, databases and devices, exposing them to a multitude of malware and Ransomware and compromise patient data.

Journal of Theoretical and Applied Information Technology
15th January 2022. Vol.100. No 1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

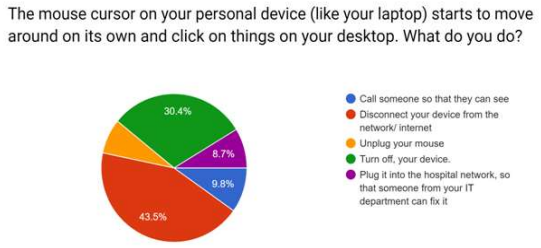

Figure 4.5.1.1: Reaction to a Breach on a Personal Device

4.5.1.2 Breached hospital device scenario

The second scenario figure 4.5.1.2 (below), was like the first, accept it was based on observance of the hacking of a hospital device. Only 53.3%, correctly elected to disconnect the device from the network and call IT, while 18.5 % elected to turn-off the device (disconnecting the device will terminate the hack on the device but may result in possible data loss and software damage and downtime. Furthermore, because the device is on the hospital network, the network and remaining connected devices are vulnerable. 28.2% selected incorrect actions would allow hack to continue unhindered and potentially spread throughout the entire hospital network and all connected devices. Again, these actions although reflected by the minority (28.2%), directly threaten the hospital network, databases and devices, exposing them to malware, Ransomware attacks and possible loss or exposure of millions of patient records. These reactions are concerning and evidence of the poor state of cyber security awareness among MIS custodians. Revealing a lack of understanding; poor knowledge of data protection; and lack of required skill, to effectively identify, minimise and/or neutralise a hacking threat. This Further substantiated, as only approximately 36% of participants knew of the common system vulnerabilities utilised by hackers, to facilitate a distributed spam attack.

Figure 4.5.1.2: Reaction to a Breach on a Hospital Device

4.5.2 Phishing, malware and social engineering threat scenario

Ransomware is a highly prevalent variety of malicious software, found in 39% of malware-in 2018. The human factor continues to be a key weakness: Employees are still falling victim to social attacks. Financial pretexting and phishing represent 98% of social incidents and 93% of all breaches investigated – with email continuing to be the main entry point (96% of cases). Companies are nearly three times more likely to get breached by social attacks than via actual vulnerabilities, emphasizing the need for on-going employee cyber security education [44].

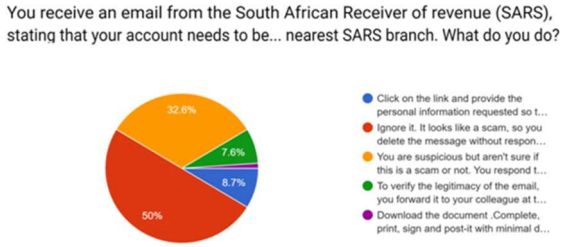

Figure 4.5.2: Reaction to a Phishing, Malware and Social Engineering Threat

The final scenario figure 4.5.2 (above) impersonated a trusted and well-known government department to mask a combination of phishing, social engineering and Ransomware (malware attacks. Half of MIS custodians correctly ignored the email, successfully obverting the attack and mitigating the threat. 32.6 % were suspicious but engaged further by replying to the email, thus increasing their exposure to the possibility of further social engineering attacks (like pretexting).

8.7% elected to click on the provided link, immediately exposing them to Phishing based attack. Typically, after clicking the link, the user is redirecting to fake website, mimicking the original. Then, the user is prompted to login and their login credentials are copied. Thereafter, the user is redirected to the original website were their re-attempted login is successful. Users typically attribute the initial failed login to a hardware/software glitch and are oblivious to the fact that their login credentials have been hacked. The hacker may (at their convenience) utilise the secure login credentials to access to personal/company systems, databases and devices. Thankfully, only a minority (1.1%) elected to download the document, which would instantly

Journal of Theoretical and Applied Information Technology
15th January 2022. Vol.100. No 1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

expose their device\system to a malware-based attack, like Ransomware. Concerning, are 8.7% elected to forward the email to a work colleague, on duty at the hospital, instructing them to download the attachment and print the attachment. The forwarded email gains instant credibility (because, it has been received by trusted fellow employee); downloading the attachment, exposes all hospital devices, systems and databases, to host of malware-based threats, like Ransomware. The scenario above, demonstrated that a skilful attack (utilising a combination of phishing, social engineering and malware), primarily targeting the personal/private device of an unsuspecting MIS custodian could directly threaten the data, devices and systems within a hospital network.

Table 4.5.2: Understanding of Terminology in Comparison to Reaction to Scenario

Correct defined terminology	Click on the link and provide the personal information requested so the security matter can be addressed immediately	Download the document. Complete, print, sign and post-it with minimal delay	Ignore it. It looks like a scam, so you delete the message without responding.	To verify the legitimacy of the email, you forward it to your colleague at the hospital- asking him/her to download and print the attachment and give you feedback.	You are suspicious but aren't sure if this is a scam or not. You respond to the text message, asking questions to determine if the situation is legitimate before you provide the information requested.	Grand Total
PHISHING	6	2	46	8	22	84
RANSOMWARE	2	0	22	6	10	40

Closer analysis of correct responses correlates with correct understanding of the threat terminology. This scenario evaluated theoretical knowledge, understanding and practical application of a simulated real-world event. The table below shows a correlation of correct responses about the attack definitions viz. Phishing and Ransomware in comparison to correct responses to the scenario.

There is a clear correlation showing 54.7% (46/84) of those that answered correctly, also correctly understood the definition of Phishing and 55% (22/40) correctly understood the definition of Ransomware. Indicating that sound theoretical knowledge of cyber threat terminology does influence correct practice.

Table 4.5.3: Correct response to threat vectors and interpretation of Ransomware

	What is Ransomware?			
Correct actioning based on the SARS Scenario-based	software that should be installed to protect against viruses	I do not know	An attack which encrypts the files of the infected system	Grand Total
Ignore it. It looks like a scam, so you delete the message without responding.	19	52	22	93

Of the 93 that answered correctly, 52 indicated that they did not know what Ransomware was, and a further 19 had an incorrect understanding of Ransomware. Only 22/93 correctly understood what Ransomware was, hence these are the only participants which are likely to have made a genuinely informed decision to protect their systems from a possible Ransomware attack. It is likely that the others merely, choose the option which was safest or offered the least exposure to a misunderstood threat vector.

Table 4.5.3: Correct Response to Threat Vectors and Interpretation of Phishing

	What is Phishing?				
Correct actioning based on the SARS Scenario-based	Disguised hyperlinks and sender â€™s addresses	I do not know	Unsolicited requests (usually sent via email) to fool receivers in divulging personal information	Viruses being downloaded onto your devices	Total
Ignore it. It looks like a scam, so you delete the message without responding.	5	30	46	4	93

Analysis of the data shows that of those whom correctly reacted to the SARs scenario question, 46/93 correctly understood the definition of phishing; and 30/93 admitted to not knowing what phishing was. Indicating that some whom correctly reacted to the SARs scenario, did not have a sound theoretically understanding of these cyber threats (viz. phishing, Ransomware) and may have chosen the option which was safest or offered the least exposure to a misunderstood threat vector. This may indicate a lack of understanding, thus the actual percentage of MIS custodians whom correctly reacted to the scenario because they understood the risk and correctly calculated their response based on their knowledge, skill and belief; is significantly lower than the indicated 50%.

The findings of this research are applicable only in the target population of the secondary healthcare institutes under study. The results that are obtained from this research study are not directly generalizable and transferable to other nursing populations. The results are restricted to the private secondary healthcare institutions because the demographic and economic factors differ, as compared to that found in other public or primary institutions. The study was further limited by allocated time and self-funding. A third constraining factor was the site of the investigation, which was limited to two private hospitals in Kwa-Zulu Natal. The hospital information security infrastructure, policies and configuration were outside of the scope of this study.

4. CONCLUSION

MIS custodians generally lack the proper knowledge of cyber security terminology, internet/online fundamentals and there is significant misunderstanding or uncertainty of common cyber threats targeting end-users within the healthcare industry (viz. social engineering, spam, phishing and Ransomware). There is also lack of understanding pertaining to current and developing legislation around the protection of electronic medical information.

MIS custodians are exposed to cyber-attack, by way of the nature and extent of their online activities, most engage in online activates which inherently create exposure to cyber-threats. Their intentions around utilisation of strong passwords, encryption, downloading, spam and online cyber practice (including software patching, utilisation of antivirus, threat vectors etc.); can be enhanced and improved. There was evidence of poor cyber practice habits when utilising personal devices; and there was enough intention supporting the cross-utilisation of devices and information, between personal and hospital networks. Therefore, it is plausible that their current personal practice and habits may impact both their personal infrastructure and hospital network and infrastructure.

The poor cyber-practice of MIS custodians was predominately inadvertent however; the current cyber-related practice and knowledge of MIS custodians, does pose both a security and legislative risk, which should be further investigated and mitigated accordingly. There was evidence supporting the intent for the utilisation of personal or private devices and/or infrastructure, to access hospital infrastructure and to utilise hospital devices and/or infrastructure to access, store and/or process personal data/activities. Evaluation of this risk is warranted, considering the poor cyber practice and exposure of personal devices, together with intended utilisation between personal and hospital infrastructure. Additionally, the uncertainty in relation to their knowledge of applicable acts and legislation pertaining to protection, confidentiality, security and disclosure of electronic medical health information; is a possible area of concern. South African law around protection of electronic information and cyber-crime is developing and growing towards global trend alignment. Many, US healthcare companies have been bankrupted (as discussed in the literature review), from an onslaught of lawsuits and reputational damage, following major data-breach/loss occurrences.

The study analysed the reaction of MIS custodians, towards abnormal cyber activity and suspicious cyber occurrences, by way of practical scenario-based situations related popular cyber threats targeting end-users within the healthcare industry (viz. social engineering, spam, phishing and ransomware). Unfortunately, the stakes around MIS are high and a major data breach/loss can result from a single incident, were a clever threat vector had exploited the ignorance of an unsuspecting individual. A significant portion of MIS custodians are unprepared to respond or recognise a cyber-threat/attack/breach. The majority are unaware new legislation, which makes reporting of certain breach/data loss incidents compulsory.

The analysis of causes of poor cyber practice or intention was predominately unintentional, stemming from misunderstanding, ignorance or unawareness. Most MIS custodians feel a responsibility to protect medical information, but most lack the necessary cyber understanding and legislative awareness to intentional support this. MIS custodians are lacking the necessary situational awareness about current cyber threats within the healthcare industry (viz. social engineering, spam, phishing and ransomware). There are significant knowledge gaps around cyber-security issues and best cyber practice. Furthermore, their perceived cyber skill and ability is significantly lower than their actual skill and ability. Some have indicated that they have attended internet/online/cyber training, however, based on the results, the scope, relevance and frequency of the training is questionable.

Globally, the current COVID19 pandemic has necessitated the importance of reliable real-time electronic patient information. In South Africa, there is a strong requirement to increase the level of security awareness of various technology users and ICT security practitioners [43]. Protecting digital information in terms of CSI is on-going battle between information accessibility and information

security. Currently, South African electronic medical information sharing is in its infancy with limited integration and interoperability. The industry is aspiring towards global trends, racing towards increased integration, national interoperability and online personalised access and management. Digital information threats are rapidly evolving; therefore, within information security auditing, a cyber-risk-based approach must be continuously applied, to support identification, evaluation and mitigation. This study has not completed an audit of the healthcare group's information systems, processes and policies; or an investigation of security, interoperability and the accessibility of their current MIS. Therefore, this study does not speculate on the impact of the findings, rather offers insight into the cyber awareness and practice of its key users, as an input into its existing information security auditing process (where the associated impact can be investigated and mitigated accordingly).

The study found significant lack of knowledge, unknowingness and misunderstanding amongst hospital MIS users, about cyber security issues. The study found evidence supporting unsafe beliefs about cyber security - contradicting best cyber practice. Some beliefs were unsafe, unconcerned or careless thereby increasing vulnerability to cyber threats. There was significant evidence indicating a lack of confidence in both individual and collective, safe cyber security practice. The study found that skills around cyber security were over-rated in comparison to actual cyber security and online skills. The combination of a false sense of self-confidence and unawareness of good cyber practice increase the probability of employee negligence and human error, which appears to be the root cause of database breach causes, globally (as discussed in Chapter 2). The study found that most MIS users felt legally responsible for patient information, however, because of their general lack of familiarity with current legislation governing information security, protection of information, electronic communication and cyber security; they unfortunately pose a significant legislative and financial risk. The impending legal ramifications of this crucial aspect solely justify the financial requirement for intervention.

The personal poor cyber security practice of respondents is alarming implying that most personal devices are vulnerable. There is significant lack of appreciation for cyber security tools and protocols. The majority engage in typical online activities including the use of social media, online shopping, gaming and streaming however, 15% access torrent websites, which are synonymous for spreading viruses. Additionally, the majority are unaware of the latest cyber security threats. The combination of these practices increases their personal susceptibility to cyber-threats. In a worst-case scenario assuming interchangeable utilisation of personal devices on hospital network and vice-versa is prevalent; the current poor cyber-related practice on personal devices, may pose a major security risk to hospital devices, data and infrastructure. In a best-case scenario assuming there is no interchangeable utilisation of personal devices on hospital network and vice-versa, there is the residual risk of poor cyber behaviour i.e. MIS custodians who are guilty of having poor cyber habits on their personal devices may continue this behaviour, when utilising hospital networks and/or devices.

The cyber practice of respondents (assessed via a scenario combining social engineering, phishing and malware) was concerning. The actions of half would expose them to phishing and social engineering-based scams, compromising their personal data and devices. More concerning, are the actions of the 8.7% that elected to redirect the threat towards the hospital, exposing hospital infrastructure and patient data. Furthermore, results obtained from the breached hospital and personal device scenarios (4.5.1 and 4.5.2), raises concerns about the behaviour of MIS custodian to minimise the scope of the breach and/or reduce data loss, from a breach incident. The cyber security practice of only 43.5% would successfully terminate breach on a personal device, reducing further data losses and spread, but alarmingly 8.7% would redirect the threat towards the hospital network. Only the actions of slightly more than half (53.3%), correctly terminated the breach on a hospital device thus minimising data loss and spread. Terrifyingly, the actions of 28% would allow the breach to spread through the hospital network, potentially exposing more hospital devices, infrastructure and incur further losses/exposure of patient data.

The relevancy, scope and frequency of those who indicated they received online/internet/cyber

training, is unknown. Results indicate that 47.2% of MIS custodians have never attended cyber security, internet security or online security training however, both formally trained and untrained hospital MIS users, lack basic knowledge around cyber security thus, there is compelling evidence supporting the necessity to up skill hospital MIS users.

Cyber security is a subset of information security and the human element was the focus of this study. Many MIS custodians may be unaware of the difference between safe and unsafe cyber practice, because disregard for basic safe cyber practices is evident; and ignorance of basic terminology, common cyber threats and pertinent legislation, is prevalent. Therefore, the findings of this study conclude – there is evidence showing poor cyber awareness among MIS custodians working in private secondary healthcare facilities. There is a strong requirement supporting the improvement of skill, ability and knowledge of hospital MIS custodians, as substantiated by significant evidence of misunderstanding about cyber and information terminology; disregard for secure/good cyber practice; poor knowledge of cyber threats and cyber threat mitigation; and uncertainty pertaining to pertinent legislation. Only, approximately half of respondents believe that the cyber practice of themselves and their colleagues, within their professional environment, is safe. Considering the combined effect of the individual evaluations about the belief, skill and knowledge of hospital MIS users, when applied to TPB, the study concludes that the perceived cyber behaviour in relation to the awareness and practice of nurses is potentially unsafe.

5. FURTHER STUDIES AND RECOMMENDATIONS

The present research has limitations, both in the methodology and scope as indicated in the findings of this study. This survey is relatively rare within the South African medical industry, but is necessary, as is paints an important picture about the human level of cyber-readiness, as more MIS systems replace traditional paper-based systems. The findings are specific to MIS custodians within the private sector of secondary healthcare, therefore this study provides a foundation for areas of inquiry around cyber practice, knowledge and awareness within healthcare; and more importantly provides the opportunity to learn and address the human aspect of MIS, from a cyber-security risk perspective. It would be extremely interesting to perform a similar survey with other hospital groups and/or between different healthcare sectors; and to compare the results, find patterns, similarities and differences among them to reach a nationwide overview of the phenomenon.

The study did not evaluate the security of MIS within the hospital from a technical IT perspective but has concluded that the state of cyber security awareness of MIS users, poses a significant risk to hospital MIS, warranting urgent intervention. Optimistically, with greater communication and cooperation between healthcare providers and researchers within this field more studies focused on SA hospital IT polices, IT strategy and existing security mitigation of cyber related threats, would extremely beneficial.

Correlation of data, from future such studies within developing countries would be useful in creating best practice guidelines and cyber training toolkit tailored towards improving cyber awareness of healthcare professionals.

In response to the increase in global cyber-attacks within the healthcare industry, a multidisciplinary team of experts met to address cyber-security in hospitals at the bi-annual Geneva Health Forum (GHF) in April 2018. The purpose of these meetings was to exchange perceived threats, to promote interdisciplinary discussion, and to propose practical recommendations for hospitals across the globe. Among the key recommendations the following pertinent aspects were highlighted [25] -:

1. *Addressing cyber-security via the product lifecycle in a preventative and proactive manner, with emphasize a quality IT foundation, stable application base and strong IT infrastructure.*
2. *The utilisation of a risk-based approach, beginning with the identification of at-risk IT assets, followed by management of trade-offs between risks and benefits, as well as different types of risks.*
3. *The importance of training end-users.*
4. *Strategies around vulnerability management, patch management and the controlled and restrictive granting of administrative privileges.*

5. *The development of incident response and business continuity plans.*
6. *Information sharing among stakeholders to build resilience.*
7. *Privacy-conscious data sharing and the unique challenges medical devices pose to security.*

The results of this study in relation to recommendation (1) fell outside of the study. However, the study recognises the advantage of the approach which will be of particular benefit to developing world. The focus on quality applications will help promote standardisation and interoperability in respect of the SA national eHealth strategy. Furthermore, the study supports the emphasis of strong IT support. Additionally, this study further recommends a strong IT focus towards the development and continuous assessment of MIS users' cyber practice and awareness.

The results of this study concur with recommendation (2), supporting the adaptation of a risk-based approach. As a result of scope limitations, recommendations presented within this study, have identified areas of concern, where such an approach may be employed to analyse the impact of the risk, then mitigate in accordance their associated risk appetite.

The results of this study in relation to recommendation (3), was found to be extremely pertinent to developing countries like SA. Considering the increasing cybercrime and planned eHealth development within SA healthcare, it is imperative that structured cyber training programs be implemented, as soon as possible. This study concurs with the *Cyber Security Readiness Report* of South African companies; recommending regular cyber training programs for beginner, intermediate, advanced and hybrid hospital MIS users [43], together with annual refresher training and assessment modules. Considering the evidence of exploitation of the human element and corresponding devastating impact associated with data breach/loss; the maintenance of safe cyber practice and education of MIS custodians requires dedicated resources. To effectively address cyber readiness, mitigation must also include on-the-job-training components and assessments (penetration testing), similar to those employed by other safety critical industries (e.g. aviation).

The results of this study in relation to recommendation (4), from a hospital IT perspective, fell outside the study scope. The cyber practice of MIS custodians, on personal devices, showed a general neglect regarding software patches, software updating and correct use of antivirus. Additionally, there was evidence supporting the intent to utilise personal devices on hospital networks and vice-versa, hence personal risk and poor practice may transfer risk to hospital IT infrastructure. Therefore, this study recommends an investigation into the inter-utilisation between private and hospital infrastructure and information sharing, employing a risk-based analysis of relevant policy (BOYD), procedure a practice; to ascertain the impact of this risk in comparison to current mitigation.

The results of this study support recommendation (5), although not entirely within study scope, because there was significant evidence of uncertainty around response to data breach /loss incidents. Hence, the study recommends a review of current incident repose and business continuity policies and procedures, with cognisance of current and developing legislation within SA. Furthermore, these plans must be communicated and demonstrated, so that MIS custodians are aware of correct action to follow when they suspect a data breach event, minimising loss and further spread.

Following the theme from (5), this study supports recommendation (6). MIS custodians are key stakeholders and must be aware of developing threats. Furthermore, the most effective mitigation against cyber threat like phishing, are regular information about new phishing strategy and ploy [27]. In the US the recurrence of past security breaches in healthcare showed that lessons had not been effectively learned across different healthcare organisations, therefore Generic Security Templates (GSTs) have been proposed to facilitate this knowledge transfer to improve learning and to share security knowledge to prevent future attacks [45]. Cyber awareness and resilience will benefit from affiliations with similar cyber security awareness groups and Computer Security Incident and Response Teams (CSIRTS); therefore, this study recommends the prompt and regular dissemination of industry specific security advisory (cyber-attack vector signatures, cyber alerts, breach, cyber threats and possible mitigations etc.) to all healthcare stakeholders (executive to MIS custodian); to build cyber situational awareness.

When stakeholders are alerted to the danger (cyber threat) and are aware of the ploy (how), the probability of a recurrence (due to human error/exploitation and/or social engineering) will be significantly reduced. The study findings concur that TPB factors (attitude, subjective norms, and perceived behavioural control), as well as collective felt trust and trust in information security technology, are positively related to compliance intention [46], thus more likely to increase cyber situational awareness and increase resilience.

The results of this study in relation to recommendation (7), found that most MIS custodians felt responsible for the protection of medical information but, there was significant lack of knowledge of pertinent legislation about patient privacy, confidentiality and protection of patient information. The study also found significant intent to utilise personal devices on hospital networks and vice-versa. Bring your own device (BOYD) practice and COVID19 motivated working from home practices have increased, therefore the study recommends an audit of all relevant policy, procedures and existing mitigation cognisant of developing cyber threats, current cyber practice and knowledge of MIS custodians and developing legislation.

REFRENCES:

[1] DOH, S., *National eHealth Strategy, South Africa 2012/13-2016/17*, S.A.D.o.H. (DOH), Editor. 2012, South Aftrica (SA) Department of Health (DOH).

[2] Society, M.P., *Medical Records in South Africa - An MPS Guide*. 2014.

[3] WHO, *Density of physicians (total number per 1000 population, latest available year).* Global Health Observatory (GHO) data, 2017.

[4] WHO. *Global diffusion of eHealth: Making universal health coverage achievable* Report of the third global survey on eHealth 2016 01/12/2016; Available from: http://apps.who.int/iris/bitstream/10665/252529/1/9789241511780-eng.pdf?ua=1.

[5] Wolfpack. *2012/13 The South African Cyber Threat Barometer*. A strategic public-private partnership (PPP) initiative to combat cybercrime in SA 2017 [cited 31 May 2017; Available from: http://www.cyanre.co.za/wp-content/uploads/2016/08/cyber-threat-barometer.pdf.

[6] Cassim, F., *Addressing the growing spectre of cyber crime in Africa: evaluating measures adopted by South Africa and other regional role players.* The Comparative and International Law Journal of Southern Africa, 2011. 44(1): p. 123-138.

[7] Symantec, *2017 Internet Security Threat Report*. 2017.

[8] Interchange, W.f.E.D., *The Rampant Growth of Cybercrime in Healthcare.* 2017.

[9] KPMG, *Health Care and Cyber Security: Increasing Threats Require Increased Capabilities*. 2015.

[10] Ponemon. *Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data*. 2016 31 MAY 2016]; Available from: http://lpa.idexpertscorp.com/acton/attachment/6200/f-04aa/1/-/-/-/-/Resources%20-%20Sixth%20Annual%20Benchmark%20Study%20on%20Privacy%20and%20Security%20of%20Healthcare%20Data%20.pdf?cm_mmc=Act-On%20Software-_-email-_-ID%20Experts%20Download%20-%20Sixth%20Annual%20Benchmark%20Study%20on%20Privacy%20%2526%20Security%20of%20Healthcare%20Data-_-Download%20Now&sid=TV2:CvNevTRM0.

[11] Team, R. *10 Biggest Cyber Crimes and Data Breaches Till Date*. 2017 2017/05/16]; Available from: https://thebestvpn.com/cyber-crimes/.

[12] A Smith, S.S.a.N.B., *Why 'WannaCry' Malware Caused Chaos for National Health Service in U.K*, in *NBC*. 2017: Online

[13] Mitrovic, Z. *Can BRICS boost cybersecurity of its member countries?* 2018.

[14] PWC, *Global Economic Crime Survey 2016 – 5th South African Edition*. 2016.

[15] Kirsten Doyle. *Data breaches remain unreported by SA organisations*. 2017 22/05/2017]; Available from: http://www.itweb.co.za/index.php?option=com_content&view=article&id=160221.

[16] van Niekerk, B., *An analysis of cyber-incidents in South Africa.* The African Journal of Information and Communication, 2017. 20: p. 113-132.

[17] Reuters, *South Africa's Life Healthcare hit by cyber attack*, in *Reuters online Newspaper*. 2020: online.

[18] Siwicki, B. 2016 [cited 2016 31 May]; Available from: http://www.healthcareitnews.com/news/ponemon-89-percent-healthcare-entities-experienced-data-breaches.

[19] Ponemon. *2016 Cost of Data Breach Study: Global Analysis*. 2016 2016 [cited 2016 June

2016]; Available from: https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094WWEN.
[20] Smith, Z.M., E. Lostri, and J.A. Lewis, *The Hidden Costs of Cybercrime*. 2020, McAfee, LLC. 4631_1220.
[21] Mcanyana, W., C. Brindley, and Y. Seedat, *Insight into The Cyberthreat Landscape in South Africa*. 2020.
[22] IBM, *IBM X-Force Threat Intelligence Index 2017*. 2017.
[23] Yee Ling Boo, D.S., Kok-Leong Ong, *Data Mining: 15th Australasian Conference, AusDM 2017, Melbourne, VIC , Austria 19 -20, 2017*. 2017.
[24] NDoH, *National eHealth Strategy, South Africa 2012/13-2016/17*, S.A.N.D.o. Health, Editor. 2012.
[25] Argaw, S.T., et al., *Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks.* BMC Med Inform Decis Mak, 2020. 20(1): p. 146.
[26] Proofpoint, *2021 State of Phish - An In-Dept Look at User Awareness, vulnerabilty and Resilence*. 2021.
[27] 27. Kim, L., *Cybersecurity and related challenges during the COVID-19 pandemic.* Nursing, 2021. 51(2): p. 17-20.
[28] Argaw, S.T., et al., *The state of research on cyberattacks against hospitals and available best practice recommendations: a scoping review.* BMC Med Inform Decis Mak, 2019. 19(1): p. 10.
[29] Bello, I.S., et al., *Knowledge and utilization of Information Technology among health care professionals and students in Ile-Ife, Nigeria: a case study of a university teaching hospital.* J Med Internet Res, 2004. **6**(4): p. e45.
[30] Mugomeri, E., et al., *Assessment of Computer Literacy of Nurses in Lesotho.* Comput Inform Nurs, 2016. 34(11): p. 528-534.
[31] Jack, C., Y. Singh, and M. Mars, *Pitfalls in computer housekeeping by doctors and nurses in KwaZulu-Natal: no malicious intent.* BMC Med Ethics, 2013. 14 Suppl 1: p. S8.
[32] Chandarman, R., *Cybersecurity Awareness of Students at a private higher education institute in South Africa*, in *School of Management, IT and Governance*. 2016, UNIVERSITY OF KWAZULU-NATAL.
[33] Systems, C.R. *Sample Size Calculator*. 2012 14 April 2014]; Available from: http://www.surveysystem.com/sscalc.htm.
[34] Ajzen, I., *The theory of planned behavior.* Organizational Behavior and Human Decision Processes, 1991. 50(2): p. 179-211.
[35] Ifinedo, P., *Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory.* Computers & Security, 2012. 31(1): p. 83-95.
[36] Naidoo, V. and B. Van Niekerk, *Strategic information security management as a key tool in enhancing competitive advantage in South Africa.* Journal of Contemporary Management, 2014. 11: p. 33-46.
[37] Sutherland, E., *Governance of cybersecurity - The case of South Africa.* African Journal of Information and Communication, 2017. 20: p. 83-112.
[38] Spence, N., et al., *Ransomware in Healthcare Facilities: A Harbinger of the Future?* Perspectives in Health information Management, 2018.
[39] Mars, M. and R.E. Scott, *WhatsApp in Clinical Practice: A Literature Review.* Stud Health Technol Inform, 2016. 231: p. 82-90.
[40] Marivate, V., et al., *Protect your personal information on Socail Media - Warns CSIR Cycbersecurity Experts*. 2018, Council for Scientific and Industrial Research website.
[41] Pagnini, P. *According to a new study conducted by researchers at Digital Citizens Alliance and RiskIQ almost one-third of the 800 torrent websites served malware.* 2015.
[42] Huckvale, K., et al., *Unaddressed privacy risks in accredited health and wellness apps: a cross-sectional systematic assessment.* BMC Medicine, 2015. 13(1): p. 214.
[43] DTPS, *Cybersecurity Readiness Report 2017*. 2017, Department of Telecommunications and Postal Services, South Africa.
[44] 44. Verizon, *2018 Data Breach Investigations Report*, in *11th Edition*. 2018.
[45] He, Y. and C. Johnson, *Improving the redistribution of the security lessons in healthcare: An evaluation of the Generic Security Template.* Int J Med Inform, 2015. 84(11): p. 941-9.
[46] Jalali, M.S., et al., *Why Employees (Still) Click on Phishing Links: Investigation in Hospitals.* J Med Internet Res, 2020. 22(1): p. e16775.