Mokata Johannes Nkwana, MS
Lecturer at University of South Africa
Department of Criminology and Security Science
E-mail: buthemw@unisa.ac.za

Prof.dr Muzukhona Buthelezi
Associate Professor at the University of South Africa (Unisa) in the College of Law, Department of Criminology and Security Science.
E-mail: buthemw@unisa.ac.za

DOI: 10.37458/ssj.3.2.1
Research Paper
Received: September 29, 2022
Accepted: November 14, 2022

SAFETY OF PUBLIC HOSPITALS IN SOUTH AFRICA: AN EXAMINATION OF SAFETY AND SECURITY MEASURES AT FIVE PUBLIC HOSPITALS IN GAUTENG, SOUTH AFRICA[1]

Abstract: *Public hospitals are regularly confronted by safety and security breaches that expose employees, patients, and visitors to serious and violent crimes such as assault, rape, murder and theft. Furthermore, assets such as computer equipment, medical files, medical equipment, and medicines are frequently stolen from state hospitals. This paper is aimed at is aimed at identifying security gaps and shortcomings in the provision of security services so that recommendations can be formulated to address the assessed risks and other threats. Furthermore, the paper described the effectiveness of safety and security measures that are currently employed in public hospitals. A qualitative study was conducted at five public hospitals in the province of Gauteng. Data was collected through one-on-one in-depth interviews with 30 key participants who were selected through purposive sampling. Additionally, safety and security documents were analysed, followed by observation of security personnel in the control rooms. The research confirmed that inadequate security systems regarding perimeter fences,*

[1] This article is based on the data gathered from the study of the author's PhD research.

closed-circuit television and trained security personnel at the research sites made it difficult to deter, detect and detain perpetrators. Furthermore, the use of a Security Risk Management Model developed specifically for public hospitals during this research is recommended.

Keywords: *examination, safety, security, security breach, security measures, state hospitals*

INTRODUCTION

Public hospitals are confronted by safety and security breaches whereby personnel, patients and visitors are exposed to crimes such as physical assault, rape, theft, pickpocketing, purse snatching and mugging (Anon, 2017). Other criminal activities faced by hospitals are cyber-attacks designed to disable the information technology (IT) and health record systems, thus resulting in many disruptions. For example, a syndicate involving various role players has allegedly been involved in the theft of medical files from Chris Hani Baragwanath Academic Hospital in Soweto, south of Gauteng. The motive for the apparent theft of medical files relates to a conspiracy between individuals from several law firms and employees from the Road Accident Fund. The Gauteng Member of the Executive Council (MEC) for Health, Qedani Mahlangu, confirmed that 12 files went missing from the motor vehicle accident file office. Five of the files were found in the boot of the vehicle of one of the suspects (Rahlaga, 2016).

As such, a review of safety and security measures at state hospitals is urgent. According to the National Occupational Safety Association (NOSA) in their specification document regarding Safety, Health and Environment Management System standards (2013), safety refers to the freedom from unacceptable risk of harm (NOSA, 2013), whereas in the context of corporate security, security is viewed as a process for protecting the business enterprise. Thus, security means freedom from risk or danger (NOSA, 2013). According to Halibozek and Kovacich (2017:48), security means anything that provides or assures safety. These two concepts are of paramount importance in state hospitals because they are both concerned with the well-being of employees, patients and visitors.

The aim of this article is to describe how the public hospitals included in the sample protect their assets, information, personnel, patients and visitors against criminal activities. Furthermore, security risks and threats associated with safety and security at state hospitals are outlined and recommendations are proposed.

LITERATURE REVIEW

Securing public hospitals is essential in any country because hospitals are always soft targets and can be easily targeted by terrorists. Attack on public hospital is not South Africa's problem but it is spread throughout the world. Boaz, Miri & Wernli (2013) produced a research paper that covered more than 100 terror events against hospitals in the period 1981-2013 in 43 countries. They found that 775 people lost their lives, and 1,217 were injured in the attacks. They further found that from January 1970 to December 2020, there were 961 attacks in 76 countries against healthcare facilities and healthcare workers. Besenyő, Márton & Shaffer (2021) added to this provision by submitting that 3,006 people died and 4,673 were injured during the attack of healthcare facilities.

Violence against staff in hospitals and healthcare institutions affects both industrialized and developing countries, and that verbal violence is as present as physical violence. Violence against medical personnel damages not only the health and dignity of employees, but also the productivity of organizations. Violence in healthcare also poses a threat to patient safety and the quality of patient care. In Sweden, 29% of health workers have experienced violence at some point; the proportion is 25% in the US and 44.7% in Turkey. According to Ráczkevy-Deák (2021), 8-38% of health workers experience some form of physical violence during their careers. The author further argues that in a 2019 survey of more than 5,000 nurses by the American Nurses Association (ANA), 59% said they had been verbally abused and one in four had been physically abused by a patient.

Attacks on the healthcare facilities are not the only problem that these facilities face, they also experience cyber-crimes. This problem was worsened by the upsurge of COVID-19 pandemic. This afforded criminals an opportunity to try and manipulate security systems as more and more people started to work from home and be dependent on computers. According to Lauver (2021),

organizations must determine the conduits and amount of access that third parties have to company assets. Assessing and controlling this access is an important consideration for business owners working with third parties. To counter cyber-security attacks, Appknox (2022) suggested the following measures that are to be put in place by medical facilities; Increase in the Adoption of Multi-factor Authentication; Adoption of Biometric Security; Push for More Effective Medical Device Cybersecurity Regulations; New Payment Innovations; Securing Electronic Health Records Systems will Become Essential; Introduction of Secure Access Service Edge (SASE) Solutions; and Advancement in Securing Connected Medical Devices.

Public hospitals in South Africa are funded by government and their health services are available to all citizens, including foreigners. Subsequently, public hospitals experience a number of risks that may cause harm to patients, employees and visitors. The risks include overcrowding, rape, murder, assault or attack, fraud and corruption related to security tenders, and theft of computer equipment and patient files (Chemick, 2017).

Physical Protection System

Physical protection systems (PPSs) refer to measures implemented for the protection of assets or facilities from criminals, terrorists, foreign intelligence services, commercial or industrial competitors, malicious people or other malevolent attacks (Govender, 2018). Physical protection systems in South Africa include the security measures adopted by various security personnel such as governmental departments to protect assets, information and people from risks and threats that could be encountered during working operations. This involves the use of different security techniques, procedures and measures that include surveillance, security personnel and other security technological devices to safeguard assets, people and information against malevolent human attacks. Govender (2018) emphasises that PPS prevents unauthorised access to the assets of an organisation through deterrence, detection and response by security personnel.

Arwui, Tshivhase and Nchodu (2016) add that a PPS integrates people, procedures, and equipment for the protection of assets and facilities against theft, sabotage or other malevolent attacks that can lead to negative consequences. Moreover, a security management system incorporated into the design addresses event-reporting issues, access control, information

protection, trustworthiness, security plan preparation, accounting, inventory, training, and qualification. An established PPS can be characterised by active and passive measures designed to safeguard personnel and to prevent unauthorised access to the facility, the equipment or installation, audit materials, information, documents, and electronic data, thus protecting all these items against industrial espionage, sabotage, damage and/or theft (Arwui, Tshivhase & Nchodu, 2016:).

The objective of a PPS is to prevent overt or covert malevolent actions, and this objective is accomplished by either deterrence or a combination of detection, delay, and response. The primary functions of a PPS are **detection**, the discovery of an adversary action such as access control; **delay,** the slowing down of adversary progress, which can be accomplished by personnel, barriers, locks, and activated delays; and **response,** the action taken by the response force to prevent adversary success. Once a PPS is designed or characterised, it must be analysed and evaluated to ensure that it meets the physical protection objectives. Moreover, a PPS system performs better if detection is as far from the target as possible, and delays are as near as possible (Govender, 2018).

Technological advancement in private security

Technology currently plays a vital role. In South Africa, there is significant and rapid advancement in security technology. These rapid advances in security technology are not only providing us with new capabilities but are also changing the way that security officers execute their work. There is increasing reliance on technology and more specifically, reliance on multiple security technology systems and layered equipment systems. Surveillance is an essential part of the most modern security approaches; however, surveillance is ineffective without the input of security personnel (Donald, 2020).

Donald (2020) adds that the use of cameras and alarms should be supplemented by the deterrent of physical security personnel, an effective response capacity and an efficient post-event process that deals with evidence handling, the prosecution of criminals and the subsequent consequences for the perpetrators. Subsequently, biometrics are used in South Africa by most organisations for access control to protect assets, information, and people by allowing only authorised persons on

the premises (Holmes, 2020). Seldon (2020) argues that technologies such as drones, radar and lasers can be used to cover large areas, and these are able to produce better results than closed-circuit television (CCTV) systems.

Crime combating strategies

In South Africa, most organisations have adopted the Crime Prevention Through Environmental Design (CPTED) as a crime prevention model. According to Kole (2015), the CPTED is described as an appropriate plan that successfully uses the environmental surroundings to decrease crime and the fear of crime in people's lives. When dealing with the CPTED, three related strategies are important. Firstly, Natural Access Control – this involves the physical security measures that are put in place to prevent criminals from gaining unauthorised entry into premises or restricted spaces. The use of natural vegetation can also be beneficial here. Lastly, Natural Territorial Reinforcement / Boundary Definition – Owners of properties or people in charge of properties must ensure that measures are implemented that are able to identify any security breach in the facility (Kole, 2015).

Security Risk Assessment

Maintaining security has become more challenging over the past years. Nowadays, a good way of identifying and assessing the security risks within an organisation is by using a process called Security Risk Assessment (SRA). According to Burmahl, Morgan and Hoppszallern (2016), 78% of hospitals conduct a physical SRA annually. Security risks emerge daily; therefore, it is appropriate that hospitals conduct the SRA at least once a year. Moreover, almost 50% of hospitals use a combination of in-house and outside security companies to conduct the SRA (Burmahl, et al 2016).

Integrated security management model

Three integrated security management models were adopted for this article. Firstly, the Global Intelligence and Security Environmental Sustainability (GISES) model that represents a conceptual framework and can be used to focus the attention of policy makers and their advisers on ways to disrupt and destroy criminal-terrorist network arrangements. The GISES model embraces the concept of knowledge management, proactive leadership, teamwork and

information sharing. By adopting the GISES model, it should be possible for intelligence and security professionals to create greater links between the public and private sectors and ensure that managers recognise the importance of safety and security management services in their working environment.

The second model, the Anti-Terrorist Business-Politico (ATBP), focuses the collaborative efforts of security professionals; hence, they are fighting against terrorism in their working environment. Moreover, the ATBP model can be viewed as a generic model that focuses on inter-governmental decision-making and can be used to formulate and implement action plans to deal with a particular threat or risk, including the consequences and the after-effects of the incident. Lastly, the Environmental and Infrastructural Risk Assessment (EIRA) model is regarded as the output of the ATBP model. The main objective of the EIRA model is to focus attention on counteracting the actions of terrorists and facilitating the coordination of security and intelligence activities with those of law enforcement personnel (Trim & Upton, 2016).

RESEARCH METHOD

A qualitative research approach was followed in this research. The researcher used qualitative research because it is concerned with understanding, naturalistic observation, and the exploration of reality (Delport & Roestenburg, 2016). Using the simple random sampling technique, five of the 33 state hospitals in Gauteng were selected. These were the Chris Hani Baragwanath Academic Hospital (in Soweto, Johannesburg South), Dr George Mukhari Hospital (in Ga-Rankuwa, Pretoria North), Tembisa Tertiary Hospital (in Tembisa, Johannesburg East), Steve Biko Academic Hospital (in Capital Park, Pretoria Central) and Kalafong Hospital (in Atteridgeville, Pretoria West). To select the 30 key participants, 6 participants were selected from each hospital, and purposive sampling was employed.

Key informants selected as part of the research sample held managerial positions and their responsibilities included the management of security within their establishments. Data was collected through one-on-one semi-structured interviews with the key participants in addition to study and observation. A documentary checklist was developed to obtain information from documents relating to the safety and security within the state hospitals. Documents such as

policies and procedures, security manuals, security posters, departmental newsletters and strategic plan documents were requested and perused to assess security risks and threats in the study sites. In addition, an observation checklist was used to obtain information from the control rooms.

A computer-based qualitative data analysis program was used to analyse the research data. This method was suitable for the current study because it assisted the researcher in transforming the research data into findings. Moreover, it helped the researcher to reduce the volume of raw information, to shift significance from trivia, to identify significant patterns and to construct a framework for communicating the essence of what the data revealed (Schurink, Fouché & De Vos, 2016).

RESEARCH RESULTS

Existing status of security at public hospitals

The research revealed that 77% of state hospitals are protected by both internal and outsourced security services. Security services are a shared responsibility between internal and external security. Most security personnel are from outsourced security companies while internal security personnel constitute a lower percentage. The research determined that outsourced security is responsible for access control at the entrances, patients' wards, restricted areas and other strategic points within state hospitals. The internal security personnel are responsible for the monitoring of the outsourced security and the management of security control rooms. Internal security personnel are also responsible for controlling the access to certain strategic areas such as the offices of management.

One-third (33.3%) of the participants indicated that they do not feel protected by the current security at public hospitals because 90% of the security is outsourced and, therefore, it is difficult to maintain consistency in regard to security. In addition, 3.3% of the participants indicated a lack of security within children's wards and stated that security officers are unable to provide protection in all wards. Participants also indicated that only security officers from the outsourced security companies are deployed in the patients' wards. However, all wards are not protected, including the children's wards from which children are frequently stolen or go missing.

Outsourced security can only provide effective security services if all security personnel receive sufficient training and monitoring. Security risks are generated through the poor salary offered to outsourced security personnel by their private company, resulting in their ineffective performance.

Security policies and procedures

The research showed that most public hospitals have security policies and procedures pertaining to the safety and security of patients, visitors, internal staff and assets in place. Public hospitals rely more on national security policy since they operate at a provincial level. Of the participants, 17% indicated that they did not develop a security policy but rather used the security policy provided by their national office. A very low percentage of participants (7%) indicated that their hospitals did not develop a security policy because such documentation was not allowed to be drafted at hospital level. In addition, 80% of the participants indicated that the state hospitals have developed their own security operating procedures (SOPs), which they use together with the security policy provided by the national office. Security policies and procedures refer to a wide variety of documents.

Security policy is the cornerstone of an institution, especially regarding safety and security measures. Security policy comprises predefined regulations that govern acceptable use of security operations, while policy-response procedures are plans or strategies that define the way in which certain events are interpreted (including how to respond to them) based on the context of the predefined regulations (Quinn, Holguin, Poster, Roach & Van der Merwe, 2019).

Sixteen percent (16%) of participants indicated that state hospitals use a service-level agreement (SLA) for managing outsourced security. This document contains job descriptions and rules and regulations to be implemented by external security personnel who are employed by the state hospital. To have confidence in services, security service providers require service monitoring, service negotiation and SLAs. Regarding the requirements for rendering security services in state hospitals, the final product needed is the specification of service in the form of the SLA. The SLAs are of paramount importance since they denote the mechanisms that specify the security

requirements for effective organisation. Consequently, a well-developed and trustworthy SLA can build confidence in security service providers (Nugraha, 2015).

Security education and training

The majority of participants (90%) explained that only induction was conducted for newly employed employees. Furthermore, participants outlined that no other awareness programmes relating to security procedures took place. A safety and security programme could be implemented by security managers when educating or sensitising employees about security policies and procedures. Security awareness includes security manuals, PowerPoint presentations, scenarios and case studies that demonstrate a return on investment (ROI) for organisations. The security awareness should be reinforced through employee orientation, continuing education and closed monitoring by security personnel.

The phenomenon by its very nature can often create additional steps in normal business functions and operations. During sessions for employee security orientation, material should be prepared and presented to new employees.

Well-trained security personnel may be able to respond to security incidents such as fire, bomb threat, unauthorised entry and other related security breaches. Appropriate training will assist security personnel in taking ownership of their responsibilities. Security training is a proactive way to keep staff 'ahead of the curve instead of playing catch-up after the fact (Burmahl, Morgan & Hoppszallern, 2016).

SECURITY MEASURES

Security personnel

All the participants (100%) indicated that security officers deployed in restricted areas of the public hospitals do not cover all strategic points because the structure of each hospital is excessively large with insufficient security personnel. The research revealed that 90% of security personnel in state hospitals is from outsourced security companies whereas only 10% consists of internal security personnel. It was indicated by the participants that only internal security personnel manage strategic areas such as entrances to management offices, and there is

inadequate staff. Security personnel can provide effective access control, patrolling and monitoring of CCTV cameras in the control room if they are properly deployed in sensitive or restricted areas.

Closed circuit television cameras

All the participants (100%) stated that CCTV cameras are installed to enhance the security of the hospitals; however, they do not cover all areas. Closed-circuit television cameras help security personnel to monitor the movement of people within the hospital premises. If the cameras are properly installed where they are needed, they also deter criminals who commit crime such as theft of hospital property. However, the research revealed that some of the installed CCTV cameras were not working due to lack of maintenance. In addition, 45% of participants mentioned that state hospitals have insufficient budgets, especially for maintenance of the security systems. An insufficient security budget results in the security system not being serviced regularly. A well-serviced security system remains effective and functional and will result in an ROI for the organisation. Furthermore, 5% of the participants indicated that there was insufficient capacity or data storage, resulting in some information not being recorded or stored in the existing security systems.

Access cards/identity cards system

Of the participants, 23% said that access cards are used for positive identification of staff. However, visitors are not issued with these cards because the hospitals do not have sufficient funds in their budget to buy the cards. Another security measure, the searching of vehicles and personnel when entering or leaving hospital premises, was discussed. Only 3% of the participants mentioned that due to negligence, security personnel sometimes do not search all vehicles and/or people entering and leaving the hospital premises.

Biometric systems

Regarding biometric systems, 26% of participants mentioned that biometric systems are used in some areas. A biometric system provides effective access control for restricted areas. An unauthorised person/s is not allowed access to areas where this type of system is installed. The

study revealed that since biometric systems are very expensive, state hospitals have not installed such systems in all restricted areas due to an insufficient budget.

Security boom gates

The research revealed that some public hospitals do not have appropriate security boom gates. Fifteen percent (15%) of the participants explained that the lack of security boom gates at state hospitals because they were not budgeted in the year 2019. Security boom gates play a vital role in security because they help security officers to prevent vehicles from entering or leaving the premises until authorisation is given.

X-ray machines

Most participants (67%) stated that state hospitals do not have x-ray machines that assist security officers in searching the possessions of visitors and personnel. The research revealed that an insufficient security budget results in much security equipment such as x-ray machines not being purchased. X-ray body scanners and x-ray baggage scanners help keep public hospitals' assets, visitors, employees, and facilities safe. Weapons, explosives, and narcotics are only some of the contraband confronting security personnel. An x-ray scanner identifies harmful organic, inorganic and metal materials. Different materials absorb x-rays at different levels.

Security awareness programmes

Only 4% of the participants indicated that security awareness programmes were conducted in their hospitals. However, the programmes were not carried out regularly. Furthermore, 1% of the participants indicated that there was frustration between the internal and the outsourced security in relation to security issues, including who should be responsible for security programmes to make staff security conscious. Security awareness is essential to the survival of all organisations, including state hospitals.

DISCUSION AND INTERPRETATIONS

Security risks associated with safety and security within state hospitals

The second identified risk to health services was cyber-attack. Almost one-third (30%) of participants indicated that this type of risk did not occur in their hospitals. Participants were aware that cyberattacks can affect patient and personnel information. The solution to this problem is that the security managers together with the IT Department should eliminate the risk of malware by ensuring that appropriate security-risk control measures such as firewalls and antivirus software are installed on all hospital computers. Medical records contain confidential information and as such need continuous protection. Malware attacks are often sufficiently sophisticated to bypass defensive IT antivirus software and thus, it is important that competences are deployed across the entire network to identify and contain the malicious activities that may harm the hospital (Antonucci, 2017).

The third identified risk was murder, with 3% of the participants indicating that personnel had been murdered in their hospitals. In October 2014, a security guard at Chris Hani Baragwanath Hospital was stabbed to death by another security guard after an argument while on duty (Gillies, 2014). Arguably, if security guards fight and kill one another while they should be providing security services and protection, the question remains whether the hospital's human resources such as nurses, doctors, management, patients and other staff are secure and safe on hospital premises.

Another identified risk comprised assaults/attacks at public hospitals. One-quarter (25%) of the participants specified that there had been several assaults/attacks at public hospitals. Public hospital employees are at constant risk of being victims of assaults or attacks while executing their duties in hospitals. Attacks also occur in hospital parking areas where their cars are hijacked or stolen. From January 2016 to 11 May 2017, it was reported that 107 hospital staff at Gauteng hospitals had been victims of attacks. Victims included doctors, nurses, nurse assistants, healthcare workers, cleaners and security guards (Chemick, 2017).

Many attacks take place at night or over the weekend and particularly occur in the Casualty Department (Chemick, 2017). Tembisa Tertiary Hospital reported the most staff attacks (16 incidents), with Chris Hani Baragwanath Academic Hospital and Dr George Mukhari Hospital each reporting seven staff attacks (Chemick, 2017). Examples include a more serious assault at

Chris Hani Baragwanath Academic Hospital in Soweto in which a nurse threatened a colleague with a knife. At Dr George Mukhari Hospital in Pretoria, a doctor was assaulted with an umbrella by a patient's relative while a mentally ill patient scratched and tried to strangle a nurse (Chemick, 2017).

Arguably, hospital management should be accountable for the safety and security of patients, visitors, staff, nurses and doctors. It is the responsibility of hospital management to ensure that competent private security providers are employed to guard the hospitals. Furthermore, hospital management together with security managers should review the security system and the security policies that govern the safety and security of the institution in order to address the identified risks.

Another security risk for all people working at or visiting a public hospital is overcrowding. Almost 100% of the participants stated that overcrowding in public hospitals is a significant risk. In 2017, it was reported that the Pholosong Hospital in Gauteng was experiencing the problem of overcrowding, with some patients receiving treatment while lying on the floor. Other patients were spending weeks sleeping on the floor in the hospital's corridors.

The Occupational Health and Safety Act, No. 85 of 1993 (OHS Act) (South Africa, 1993) requires that employers should provide employees with a healthy working environment that is free from danger and hazards. It is the responsibility of the public hospital management to ensure that patients receive not only appropriate health services but also appropriate psychiatric health services and specialised facilities if required. There is a need to provide adequate medical/hospital facilities for areas demonstrating high population densities and ensure that the requisite security and safety measures are in place (Fayers, 2017).

Patients at the Chris Hani Baragwanath Hospital in Soweto, Johannesburg can expect to wait five hours to receive a file, see a doctor and obtain their medicine. In addition, there is a serious concern that Priority 2 casualty patients wait on average 69 minutes for assistance. The long waiting times are due to high patient volumes, burden of diseases, defaulting patients and staffing

in relation to patient volumes. These waiting times are unacceptable and add extra suffering for sick people (Mbatha, 2019).

In the same year, three cases of attempted rape were reported in the same hospital. After these incidents, there was a call by the Gauteng MEC for Health for security measures at public hospitals to be improved (Bloom, 2014). Moreover, in 2016 at the Lenasia South Community Health Centre in Johannesburg, an 18-year-old woman was raped in the bathroom. Despite the seemingly tight security at the clinic, the man who allegedly raped the teenage girl managed to escape. The incidents occurred while there was CCTV surveillance in place and security officers on the premises (Shange and Alexandra, 2017).

In addition, an 11 years old girl was raped at Dora Nginza hospital in Port Elizabeth. The child was brought to the hospital for medical care when she was taken to the toilet and raped. Security officers came to the scene after they heard her screaming and it was too late because the crime was already committed (TMG Digital, 2017). Arguably, hospital management wait for incidents to occur before they consider any improvements to security. In addition, more effective security and CCTV surveillance cameras and footage could be used during the investigation of security breaches.

Significant risks in state hospitals involve fraud and corruption. One-half (50%) of the participants indicated that fraud and corruption regarding security tenders is a significant problem. The phenomenon is compounded by conflicts of interest, information irregularities and lack of or inappropriate regulation at state hospitals. In most instances, fraud and corruption involve internal employees or resigned employees (Rispel, De Jager & Fonn, 2015). Over the past five years, there have been a number of fraud and corruption cases recorded at Gauteng state hospitals. One case recorded allegations of fraud and corruption involving the security contracts of Gauteng hospitals amounting to R500 million (Bloom, 2017). The following security contract cases were found to be awarded irregular by forensic audit:

- Charlotte Maxeke Johannesburg Academic Hospital: Contract amount to R33.00 million in 2016
- Helen Joseph Hospital: Contract amount to R17.00 million a year

- Chris Hani Baragwanath Hospital: Contract amount to R28.00 million a year
- Steve Biko Academic Hospital: Contract amount to R20.00 million a year
- George Mukhari Hospital: Contract amount to R16.00 million a year
- Far East Rand Hospital: Contract amount to R18.00 million a year
- Kalafong Hospital: Contract amount R15.00 million a year (Bloom, 2017).

A similar incident occurred at Pholosong Hospital in which a part of the ceiling collapsed in the maternity ward and an employee was injured (Anon, 2017). Moreover, a roof collapsed at Charlotte Maxeke Johannesburg Academic Hospital in Johannesburg; the number of injured people was not confirmed (Hlatshaneni, 2017). Arguably, hospital management or maintenance units should attend to the failing ceilings and roofs before more serious damage is caused by their collapse on patients, nurses and doctors.

Overall, the question remains whether state hospitals in Gauteng have adequate and appropriate security risk control measures in place. The short answer to this question is that the security systems currently in place at state hospitals are woefully inadequate and ineffective. Awareness of security control measures could help address incidents in health facilities.

RECOMMENDATIONS AND CONCLUSION

An examination of the safety and security measures at state hospitals in Gauteng provided the backdrop for this article that aimed to provide recommendations for improving security in the health sector.

Taking into consideration the identified security risks and threats that occurred at public hospitals, the current security systems implemented in public hospitals are ineffective and inadequate in terms of physical security measures. Furthermore, to deal with the risks associated with acts of theft, assaults, violent attacks and other criminal acts, hospital security managers should ensure that all appropriate and requisite security risk control measures within a fully integrated hospital security system are put in place. In addition, the management of state

hospitals should support the implementation of a proper security plan that incorporates a funded budget for security.

The management of public hospitals should ensure that they employ sufficient internal security personnel to monitor the outsourced security and to render other security functions such as conducting security awareness programmes. Moreover, security awareness programmes should be implemented regularly to capacitate all employees with knowledge on security policy and procedures so that security breaches can be reduced. Security awareness programmes are the responsibility of security managers; however, other sectional managers within the state hospitals should support these programmes for effective security.

In addition, the management should ensure that a security-system maintenance plan is available and effective and should provide sufficient funding for maintenance such as repairing all CCTV cameras that are out of order so that the system can operate effectively. Security systems should also have sufficient data storage to prevent the loss of valid information that would help state hospitals during investigations should security breaches occur.

To avoid security breaches from occurring within state hospitals, access control should comply with the Control of Access to Public Premises and Vehicle Act, No. 53 of 1985. Furthermore, the searching of all vehicles and people entering and leaving hospital premises should take place 24 hours a day without compromise. State hospitals should ensure the procurement of an electronic access-control system for cars. Appropriate security boom gates should be installed at the main entrances and exit gates of the hospitals to assist security officers in performing their access-control duties.

Moreover, public hospitals must implement focused security programmes for employees and management to protect information and assets from theft or compromise. Employee awareness of the problem, alertness to indicators of suspicious activity and willingness to report such indicators to management are key to the successful protection of information. The channel for reporting security incidents should be clear to all employees. An open-door policy for reporting

crime that disturbs the activities or functions of the institution should be created by hospital management.

The general lack of security at public hospitals remains one of the most serious security threats confronting the health sector. Furthermore, the non-adherence to prescribed access procedures is problematic because it allows unimpeded access to high-risk areas within the hospitals. The recommendations and findings of this article can aid academic institutions in developing study materials and guides, thus adding value to the existing body of knowledge.

REFERENCES

Anon. (2017). *World patient safety day 2017.* 17 September. Available at: http://www.gov.za/ [Accessed on: 23/06/2017].

Anon. (2017). Parts of ceilings collapse in wards at Tempisa and Pholosong hospitals. *TimesLive,* 22 July. Available at: https://www.timeslive.co.za/news/south-africa/2017-07-22-parts-of-ceilings-collapse-in-wards-at-tembisa-and-pholosong-hospitals/_____[Accessed on: 03/10/2020].

Antonucci, D. (2017). *The cyber risk handbook: Creating and measuring effective cybersecurity capabilities.* Canada: John Wiley & Sons, Inc.

Appknox. 2022. Top Healthcare Cybersecurity Trends for 2022. Available at: https://www.appknox.com/hubfs/Ebooks%202022/Top%20Healthcare. [Accessed on 26/10/2022].

Arwui, C.C., Tshivhase, V.M. & Nchodu, R.M. (2016). Modeling a physical protection system for the 444 TBq 60Co irradiation source at the Center for Applied Radiation Science and Technology, Mafikeng, South Africa. *Journal of Physical Security*, 9(1):54.

Besenyő, J., Márton, K., Shaffer, R., 2021. Hospital Attacks Since 9/11: An Analysis of Terrorism Targeting Healthcare Facilities and Workers, Studies in Conflict & Terrorism. 2021, pp 1–19. DOI: 10.1080/1057610X.2021.1937821.

Bloom, J. (2014). Safety at Helen Joseph questioned. *Politicsweb,* 3 October. Available at: https://northcliffmelvilletimes.co.za/185253/safety-at-helen-joseph-questioned/ [Accessed on 17/10/2020].

Bloom, J. (2017). R500 million irregular security contracts extended at Gauteng hospitals. *Politicsweb,* 6 July. Available at: https://www.politicsweb.co.za/politics/r500-million-irregular-security-contracts-extended [Accessed on: 11/10/2020].

Boaz, G., Miri H., Wernli, 2013. Terrorist Attacks against Hospitals: Case Studies, Working Paper no. 25, Herzliya: International Institute for Counter-Terrorism. p 4.

Burmahl, B. Morgan, J. & Hoppszallern, S. (2016). Announcement of prevention: Survey shows hospitals beefing up training to address security concerns. *Trustee*, 69(10):13-16.

Chemick, L. (2017). Spike in attacks on Gauteng hospitals staff. *IOL News*, 11 May. Available at: https://www.iol.co.za/news/south-africa/gauteng/spike-in-attacks-on-gauteng-hospital-staff-9058111 [Accessed on: 24/06/2017].

Child, K. (2017). Babies are not safe from kidnappers due to a lack of security outside maternity ward. *SowetanLive*, 05 July. Available at: https://www.sowetanlive.co.za/news/2017-05-07-count-the-ways-sa-state-hospitals-are-badly-managed/ [Accessed on: 17/10/2020].

Delport, C.S.L. & Roestenburg, W.J.H. (2016). Quantitative data-collection methods: Questionnaires, checklists, structured observation and structured interview schedules. In A.S. de Vos, H. Strydom, C.B. Fouchė & C.S.L. Delport, eds. *Research at grass roots: For the social sciences and human service professions* (pp. 171-205). Pretoria: Van Schaik.

Donald, C. (2020). CCTV surveillance needs are critical in defining types of camera development. *Hi-Tech Security Solutions*, 26(15).

Fayers, F. (2017). Hospersa highlights dismal health standards at Gauteng hospital. *Hospersa*, 8 June. Available at: https://www.hospersa.co.za/news/hospersa-highlights-dismal-health-standards-at-gauteng-hospital/ [Accessed on: 03/10/2020].

Gillies, V.C. (2014). Security guard stabbed to death. *Eyewitness News*, 05 October. Available at: https://ewn.co.za/2014/10/05/Security-guard-stabbed-to-death [Accessed on 17/10/2020].

Govender, D. (2018). *Managing security information incidents, threats and vulnerabilities: A practical approach for security practitioners serving private and government entities in South Africa*. Pretoria: Unisa Press.

Halibozek, E.P. & Kovacich, G.L. (2017). *The manager's handbook for corporate security: Establishing and managing a successful assets protection program.* 2nd edition. Chennai: Candice Janco.

Holmes, J. (2020). Global security industry adopts servistisation models. *Hi-Tech Security Solutions*. 26 (33).

Hlatshaneni, S. (2017). More details on shock charlotte maxeke hospital roof collapse emerge. *The Citizen* , 2 March. Available at: https://citizen.co.za/news/south-africa/1445217/more-details-on-shock-charlotte-maxeke-roof-collapse-emerge/ [Accessed on: 17/102020].

Kole, O.J. (2015). Partnership policing between the South African Police Service and the private security industry in reducing crime in South Africa. Unpublished dissertation. University of South Africa, Pretoria.

Lauver, M.2021. Five trends in healthcare cybersecurity. Washington DC: Security magazine.

Mbatha, N. (2019). DA slams five hour waiting time at Chris Hani Baragwanath hospital. *African News Agency*, 2 October. Available at: https://www.iol.co.za/news/politics/da-slams-five-hour-waiting-time-at-chris-hani-baragwanath-hospital-33857447 [Accessed on: 1711/2019].

National Occupational Safety Association 2013. Available at: https://www.omicsonline.org/societies/nosa-national-occupational-safety-association/ [Accessed on: 19/10/2020].

Nugraha, Y. (2015). Security assurance requirements engineering (stare) for trustworthy service level agreements. In: *2015 IEEE 23rd International Requirements Engineering Conference (RE)*. (August 2015) pp. 398-399. IEEE. Available at: https://ieeexplore.ieee.org/abstract/document/7320458 [Accessed on: 03/10/2020].

Quinn, R., Holguin, N., Poster, B., Roach, C. & Van der Merwe, J.K. (2019). WASPP: Workflow automation for security policy procedures. In *2019 15th International Conference on Network and Service Management (CNSM),* Halifax, NS, Canada, 2019, pp. 1-5. IEEE. Available at: https://ieeexplore.ieee.org/document/9012707 [Accessed on: 03/10/2020].

Ráczkevy-Deák, G. 2021. Violent acts against healthcare institutions and workers in Hungury. Contemporary Military Challenges, November 2021 (23: 4).

Rahlaga, M. 2016. Two health officials busted for suspected fraud at Chris Hani Bargwanath Hospital.EyewitnessLNews, 29 September. Available at: https://ewn.co.za/2016/09/29/Two-health-officials-busted-for-suspected-fraud-at-Chris-Hani-Baragwanath-hospital [Accessed on 17/10/2020].

Rispel L.C., de Jager P. & Fonn S. (2015). Exploring corruption in the South African health sector. *Health Policy and Planning*, 31(2):239-249. 22 June. Available at: https://www.rhap.org.za [Accessed on: 03/07/2017].

Seldon, A. (2020). You have to know it to manage it. *Hi-Tech Security Solutions*. 26 (18).

Schurink, W., Fouché, C.B. & De Vos, A.S. (2016). Qualitative data analysis and interpretation. In A.S. de Vos, H. Strydom, C.B. Fouchè & C.S.L. Delport, eds. *Research at grass roots: For the social sciences and human service professions* (pp. 397-423). Pretoria: Van Schaik.

Shange, N. & Alexandra, P. (2017). Half a million spent monthly on security at clinic were teen was raped. *TimesLive*, 08 June. Available at: https://www.timeslive.co.za/news/south-africa/2017-06-07-teen-raped-in-toilets-at-lenasia-south-clinic/ [Accessed on: 17/10/2020].

South Africa. (1985). Control of Access to Public Premises and Vehicles Act, No 53 of 1985. Available at https://www.saps.gov.za/resource_centre/acts/downloads/juta/a53of1985.pdf [Accessed on: 03/10/2020].

South Africa. (1993). Occupational Health and Safety Amendment Act, No. 181 of 1993. https://www.gov.za/sites/default/files/gcis_document/201409/act181of1993.pdf [Accessed on: 03/10/2020].

South Africa. (1998). *Minimum information security standards*. Available at: https://www.right2info.org/resources/publications/laws-1/SA_Minimum%20Information%20Security%20Standards.pdf [Accessed on: 17/10/2020].

TMG Digital, (2017). *Child raped at a hospital*. Times Live, 12 June. Available at: https://www.timeslive.co.za/news/south-africa/2017-03-15-child-raped-at-a-hospital/ [Accessed on: 17/10/2020]

Trim, P. & Upton, D. (2016). *Cyber security culture: Counteracting cyber threats through organizational learning and training.* New York: Routledge.