



EFFECT OF RISK PREVENTION TECHNIQUES ON THEFT IN PUBLIC HOSPITALS IN EMBU COUNTY, KENYA

Henry N. Otiso¹, *Department of Business Administration, Chuka University P.O Box 109,60400, 0722349519, hotiso66@gmail.com*

JohnMutugi², *Department of Business Administration, Chuka University, P.O Box 109, 60400, jmutugijohn@gmail.com*

ABSTRACT

Majority of Kenyan people receive health services from public hospitals. There is a need then to ensure that personal and hospital properties as well as people are fully protected from theft. To guarantee this protection, public hospitals have adopted risk prevention techniques aimed at reducing the frequency and severity of theft incidences. Unfortunately theft in public hospitals has become a common problem with statistics showing that hospital theft stands at 61% compared to other hospital crimes in Kenya. Cases of stolen medicine, hospital equipments and stolen babies are being reported almost now and then. The purpose of the study was therefore to determine the association of risk prevention techniques on theft in public hospitals. The study adopted a descriptive research design. The population of the study was 1608 staffs. A sample of 161 junior staff was obtained and a complete census of 56 senior staff was done. Data was collected using questionnaires. Data was analyzed using frequencies and percentages and the results presented in cross tabulations. Chi-square was used to test the hypothesis. Statistical Package for social Sciences (SPSS) facilitated the analysis. The results revealed that most public hospitals had adopted various techniques aimed at reducing theft in hospitals. The results further revealed that there was a significant association of risk prevention technique with theft in public hospitals since results obtained p value $0.046 < 0.05$ and chi-square value of 20.00 at 5% significance level. This study will form a basis of policy formulation on risk control techniques and theft matters in public hospitals in Kenya and also provide a basis for further research in field.

Keywords: Risk Management, Risk Prevention, Theft, Insurance, Hospitals



INTRODUCTION

1.1 Background Information

Theft is a worldwide phenomenon that appears to have defied efforts to contain it across the globe. Theft causes damage and fear that affects the life and well-being of people. Theft control techniques are meant to reduce theft cases and offer safety to the general public. Theft in Hospitals is common with hospital property and patients fall victim to theft. The scale of theft to personal possessions and hospital property going missing in public hospitals is depressing, and losses run into millions every year (Ministry of Health Report, 2014). When theft occurs it disrupts co-existence and results to poor delivery of health services (Kimama, 2011). Theft is a threat to people's health, government budget, hospital revenues and competition within legal industries (Lindstrom, 2007). Ignoring theft will not make the risk to go away but limits institutions from achieving their set objectives.

Since 1989, there has been an upsurge in international efforts to ensure a more secure world by adopting risk control techniques. Most public hospitals have adopted various risk control techniques that should prevent, transfer or retain the risk. Theft threat is prevented by instituting techniques such as CCTV cameras, Finger print checks using biometrics, safety audits, unauthorized entry at entry points, security alarms, Burglar proofing, security guards and perimeter fencing. Safety against losses in hospital property is also ensured by retaining risks through captives and reserves, current expensing or borrowing. Theft risk can also be transferred through insurance, leasing or hold harmless agreements. These controls make Hospital environment safer by restricting theft incidents. However Mwenda (2015) notes that most times these control techniques in institutions are defeated, ineffective or extremely expensive to buy.

Theft in hospitals is a significant problem in the world according to a report by the Global Security Index from the Institute for Economics and Peace 2014. This report further reveals that within a single year the world had experienced a 61% increase in hospital theft incidents with the number rising from 11,133 million in 2013 to 17,958 million reported cases in 2014. This report indicates that theft cases in Hospitals escalate each year despite various risk control techniques being installed in hospitals. In the united states, united kingdom and Asia along with other Nations, valuable property that were frequently stolen included wheelchairs, walking sticks, hearing aids and glasses, medicines, Laptops, children and children toys, money among other things. Public hospitals have always been easy targets for thieves and vandals because valuable items are stored in the hospitals over a long period and locations are easily approachable both night and on weekends (Human Security Report, 2014). Hospitals however have adopted various theft control techniques such as surveillance systems, security guards, perimeter walls, reserves, insurances among others aimed at reducing losses associated with theft (Dorfman, 2005). Hubbard (2009) notes that risk control techniques if fully employed could reduce the frequency and severity of theft in hospitals. He further recommends that theft control techniques need to be fully employed to ensure a safer hospital environment.



Hospitals in Africa have experienced significantly high levels of theft over the past years which have crippled the health sector. A report by the Healthcare International Association for Safety and Security (2014) representing over 10000 hospitals and healthcare facilities in Africa revealed a whopping 75% increase in theft incidents per hospital over a five-year period. Hospitals in South Africa are rated as the best in Africa with majority having adopted various risk control techniques and with theft cases being minimal. Namibia hospitals are rated the worst with the hospitals reporting to have fallen prey to thieves who are dressing as hospital workers or service company employees and stealing expensive medical equipment and valuable properties (Lindstrom, 2007). The most frequent and severe theft incidents in Africa Hospital include theft of babies, medicines and Hospital equipment. The most targeted properties are laptops and electronic gadget's used by hospital staff, which can be translated to mean millions of people's personal details and medical records are falling into the hands of criminals (Sausser, 2007).The theft incidents could have been controlled by equipping hospitals with security guards, Surveillance systems, and Perimeter walls and also losses could have been reduced through employing risk transfer and retention techniques (McKinney, 2000).

A majority of Kenya's population receives healthcare services from public hospitals. The range of services provided include preventive, promotive, curative and rehabilitative (Ministry of health, 2014).Regardless of this, Kenya has remained highly rated in hospital crime with theft being the most common crime recording a 66% which is almost twice the global average of 34% (Vander, 2014). In 2013 the Kenyan government through the Ministry of Health commissioned a survey on theft in public hospitals to be done in response to the overwhelming theft cases reported in public hospitals. The worst rated hospital in theft included Pumwani hospital, Kenyatta National hospital, Embu level five hospital and Nandi hospital. The most reported theft incidents in Kenya were medicine theft, equipment theft, personal property and money. Baby theft cases were also common(Ministry of health, 2013).Hospitals in Kenya have adopted various techniques aimed at preventing or reducing the losses associated with theft. Ochieng 2014 on his research on Control of crimes in hospitals notes that the risk control techniques are either defective or insufficient and sometimes hospitals do not pay premiums to insurance companies despite having various covers against theft. Ochieng further notes that most hospitals in Kenya are either uninsured or seriously under insured.

Young (2014) on his research on Hospital staff perceptions on theft noted that institutions including hospitals had embraced theft control techniques in pursuit to reduce the frequency and the severity of theft occurrence. According to Mwenda (2015) these techniques may be in an organization but be not effective when matters of theft are treated casually by hospital staff, patients and visitors. It is for these reasons therefore that this study aimed at establishing the effect of risk prevention techniques on theft in public hospitals in Embu County, Kenya.



1.2 Statement of the Problem

Hospitals are integral part of health care systems and theft in hospitals means a threat to global health security .Over the past years, the magnitude of theft in hospitals in the world has been on the rise (Beigelman, 2013). The government of Kenya recognized the growing threat of theft in Hospitals in early 2014 after publication of a national wide information report by the Kenya police which stated that 73% of theft incidents were reported in hospitals, followed by city street theft at 20%. According to Ministry of Health survey (2013) the most reported theft incidents in Kenya public hospitals were medicine theft, equipment theft, personal property of patients and money. Baby theft cases were also very common. This survey rated Embu General Hospital among hospitals with most frequent and severe theft incidents. Although adoption of risk prevention techniques is on the rise in hospitals, these institutions are experiencing complex theft risks with hospitals losing millions and this is threatening the safety environment in hospitals. The risk prevention techniques are designed to detect, prevent, and identify theft thereby minimizing the risk and loss to an organization. They are expected to offer a safe environment for employees, patients, visitors and hospital property. However risk control tools can be in an organization but be not effective when they are not properly developed and administered. For this reason, the researcher therefore sought to evaluate the effect of risk control techniques on theft in public hospitals.

1.3 Objective

The objective of this study was to determine the effect of risk prevention techniques on theft in public hospitals in Embu County, Kenya.

1.4 Hypothesis

The study hypothesized thatRisk prevention techniques have no significant association with theft in public hospitals in Embu County. The hypothesis was tested at0.05%level of significance.

1.5 Significance of the Study

The complexity of theft risks present strong challenges to organizational management, one of the most important being how to coordinate handling theft risks across areas within the organization. Thus, there is need to access adequate multidimensional awareness on theft related issues. The outcome of this study is essential to the administration of hospitals because it established the relationship between risk prevention techniques and the magnitude of theft. This will enable hospitals make informed decision when formulating new policies and procedures on theft risks hospitals are exposed to. The findings of this study also contributes toward building a risk-smart environment that allows for innovation and responsible risk taking while ensuring legitimate precautions are taken to protect the interest of all stakeholders. The findings of the study also informs the government, community and the general public on the nature of risk control techniques adopted and the effect they have on



controlling theft in hospitals. The researchers and academicians will also use the findings of this study to carry out related studies and use the document for further reference.

1.6 Scope of the Study

This study was carried out in public hospitals in Embu County. Embu County borders Kirinyaga County to the west, Kitui to the east, Tharaka Nithi to the north and Machakos County to the south. The study focused on risk prevention techniques employed in all the five public hospitals in Embu County. A master list of hospitals maintained by the Ministry of health compiled in May 2014 shows that there were five public hospitals in Embu County namely, Kianjokoma sub district hospital, Mbeere district hospital, Ishiara sub district hospital, Runyenjes district hospital and Embu General Hospital. Health centers and dispensaries were excluded because their operations were managed by the main hospitals. This study was confined to the senior staffs and the junior hospital staffs. Part-time and casual employees, Patients and visitors were excluded from the study because they were not permanent in hospitals hence were not well able to rate the effect of risk control techniques on theft.

2. LITERATURE REVIEW

2.1 Theft in Hospital

Hospitals are traditionally perceived as institutions that historically resisted becoming victims of insecurity whereby more efforts were put on offering services based on open and friendly access by the public. This has been practiced for decades implying that hospitals should be open 24 hours a day and seven days a week and people of any type walk in and out without being stopped. Such traditional practices have been reversed following continuous criminal threats that have resulted into dropping of the open door policy in hospitals (Aldridge, 2006).

Hospital security departments and staff are usually obliged to offer a safe environment for employees, patients, and visitors. This is attributed to the open door policy of being open and accessible to the public always which is likely to favor entry of perpetrators of crimes and other dangers to the hospital if not properly protected (Schneider, 2008). Traditional risk control techniques including the use of local tools like arrows and bows may not offer standard protection to the health care facilities. Such institutions may experience complex theft risks like infant abduction, extortion and reputation risks especially when an incident occurs (Matheson, 2010).

Security managers face unique challenges especially those related to hospital security needs affecting patients, employees and other assets which have always served as a hindrance in securing environment of care bearing in mind that no hospital is without a risk (Vellani, 2006). Hospitals are required to meet their security needs through security risk management which is essential for all hospital security managers. Such managers are charged with prioritizing the



identified risks, developing an effective hospital security plan and ensure risk reduction to manageable and acceptable levels (Warner, 2003).

Study conducted by Tim (2004), reported that 82% of the nurses surveyed in the United States had been stolen from during their careers, while 80% of the cases on registered nurses were not reported. This shows that there is growing incidence of security issues including assault, yet little about health care security is known to the public and few countries across the globe are committed to offering specific deterrents for theft professionals including nurses among others.

Theft accounts for a significant component of all hospital crimes. According to Tim (2004) effects of theft can range from irritating to devastating, both personally and financially particularly if it's on basic needs. Theft in hospital can result from insider or outsider. Security analysts have found that as many as 30% of a nation's workforce will at some point steal from their employer (Sausser, 2007). According to Mawby (2006) hospitals where staff and management have negative working relationships may have higher rates of employee thefts than where these relationships are positive. Once a theft incidence has occurred there is little chance of catching the offenders or recovering stolen property.

The magnitude of theft problem in hospitals is enormous. Identity fraud was identified as one of the top priorities of the Government of Kenya through Ministry of Health, just prior to the terrorist attacks of Alshabaab. The impact of all forms of theft is reaching a level of sophistication by criminal element thus prompt coordination by governments, multinational corporations, and citizens is required if there is going to be any significant positive impact. The Most common reported theft incidences in hospital are burglary, robbery, larceny, shoplifting and medical identity theft (Ochieng, 2014).

2.1.1 Burglary

According to the penal code a person commits burglary offense if, without the effective consent of the owner, the person: enters a habitation, or a building (or any portion of a building) not then open to the public, steals or remains concealed, with intent to steal. Factors that motivate individuals to commit burglary in hospitals are fairly common and consistent (Cromwell and Olson, 2006). The need for money is the primary reason offered by hospital burglars. This is illustrated by the burglary incident in St. Francis Hospital in Flower Hill on Long Island where a man opened offices, removed an amazon kindle and undisclosed amount of money. Rengert and Wasilchick (2000) conducted a study on sub urban burglary and found out that burglars most often strike on week days when even routinely occupied offices may be empty. According to Wright & Decker (1994) burglars selects targets based on a number of key factors: familiarity with the target, convenience of the location, occupancy, visibility or, accessibility, vulnerability or security and potential rewards.



Burglary risk control techniques include Alarms and CCTV Cameras which are undoubtedly the most effective deterrent against burglary. Burglars don't want to be seen or heard so setting off an alarm and attracting attention is their enemy. Doors are often targeted by burglars so it is important they are well constructed with good locking hardware. Outbuildings are often targeted because of their lower security. They are often located in secluded locations and contain valuables. Lighting is a proven deterrent against crime. Burglars are less likely to break into a home or any institution if it has an external light fitted front and rear. Valuables such as computers, cell-phones; GPS devices are best stored out of sight and away from windows. Locks should also be changed at least twice per year (Mwenda, 2015). This implies that hospitals need to install alarms, CCTV cameras, proper construction of walls and door, proper lighting and ensure that outbuildings are guarded at all times. This will very much help to control burglary in Hospitals.

2.1.2 Robbery

Robberies typically present the greatest risk of violence to hospital staff and the general public. This can be illustrated by a May 2015 armed robbery at a New London pharmacy that put the hospital on a partial lock down when a robber pointed a gun at employees and demanded money and pills. Crocker and Tennyson (1999) recommends that making a hospital a more difficult target will help protect the staffs from possible violent situations and provide a safer environment for the general public and the patients.

In order to prevent robbery Crocker and Tennyson (1999) recommends that hospital personnel should dress neatly and keep the working places neat and clean. Tidy and orderly premises are inviting to customers but not to robbers. Hospital environment should be well lit and any burned-out bulbs replaced. Making eye contact and offering customers a friendly greeting as they enter the facilities reduces the chances of robbery happening (Dimkov, 2009). The hospital management should encourage the police to stop by periodically. In case a robbery happens within the hospital Fischer & Green(2004) recommends that victims should scream as loudly and long as possible, and run to the nearest well-lit area, don't chase or follow the robber. If someone grabs your purse, deposit bag, or other property, do not resist, try to remember the description and mannerisms of the attacker (Dimkov, 2009).

2.1.3 Larceny

Larceny is the unlawful taking of personal property with intent to deprive the rightful owner of it permanently. To prevent larceny Knafla (2003) suggest that patients should avoid placing their purse or jacket over the back of the chair while waiting to be served. Purse should be kept on the lap or between the feet with the handle around the leg of a chair foot. Cell phones, laptops, or tablet should not be left unattended on the table and atwork; staff should put their purse or wallet in a drawer or under a desk.



2.1.4 Shoplifting

Sennewald (1992) categorizes acts of shoplifting as either rational or non-rational. While rational thieves are motivated by profit or gain, the behavior of non-rational shoplifters may be symptomatic of psychological issues and stressors. Majority of shoplifters are motivated by profit or gain and crimes are typically opportunistic. Common shoplifter traits include: nervousness or unusual actions of any kind, aimlessly walking up and down hospital premises, staying or loitering longer than usual, handling many items of merchandise, dropping articles on the floor, concealing merchandise in any way and asking numerous questions or refusing the clerks help. Others focus on looking into surveillance mirrors at the sales clerk or other customers instead of the merchandise.

Fischer & Green (2004) advises hospitals to employ effective shoplifting prevention schemes such as CCTV and EAS tagging, and most importantly, employee awareness and education. Other elements of shoplifting prevention programs may include, the enforcement of strict stock monitoring procedures, banning known shoplifters from the store and the implementation and communication of strict store policies indicating what to do when shoplifting is detected and how to detain a suspect (Fischer & Green, 2004). Possible solutions also include provision of adequate lighting, eliminating blind spots, where appropriate, utilizing security staff, convex mirrors, tags, locks and chains, post signs, warning that shoplifters will be prosecuted and maintaining a neat, orderly store with tight inventory controls (Sennewald, 1992).

2.1.5 Medical Identity Theft

Identity theft is illegal use of someone else's personal identification information in order to get money or credit. Medical identity theft has been called one of the fastest growing crimes in the world (Biegelman, 2013). Its impact can range from simple inconvenience to legal woes, financial devastation, even death. Medical identity theft can take many forms: it may involve the large-scale theft by computer hackers, it's also a crime of opportunity that can happen when your wallet is stolen and the thief uses your insurance card; or a friend or family member who has access to your personal information, use it with or without your knowledge to gain access to healthcare (HIMSS, 2012). Healthcare Information and Management Systems Society (2014) reports that signs that may indicate medical identity theft occur when: an individual receives an explanation of benefits statement listing services or treatments they never received, he or she receives a bill for services or equipment they never received, an unpaid medical bill sent by the medical provider, but it is not related to any service received by the covered individual. Also when a patient is denied health insurance benefits or prior approval for a procedure because the health insurer has claims history for that individual indicating the benefit in question has been exhausted, while this is the first time the patient is attempting to access the benefit or when a physician notes inaccuracy in historical information in medical record based on information being provided by the patient during current encounter.



Specific hazards found in healthcare settings include: unauthorized access to open workstations by both employees and outside individuals, unauthorized access to file storage cabinets or closets by employees and outside individuals and Loss or theft of physical media or devices. These include laptops, mobile phones, tablets, backup tapes, thumb drives, CDs, basically any device or media that can store electronic data (Biegelman, 2013). Privacy and security training, employee screening, biographical authentication and correctly identifying patients facilitates, efficient administration of healthcare payments allowing providers to seek reimbursement from health plans and from patients for self-pay balances hence mitigating identity theft(Crocker and Tennyson, 1999).

2.2 Effects of Theft

Successful theft can cause varying degrees of disruption to the operations of large businesses, as well as embarrassment or lost customers (Siegel, 2008). Theft represents a direct threat to the viability of smaller businesses. A theft incidence can interrupt a hospital operation quite severely, lead to workers being laid off, and in severe cases lead to institution collapsing. In addition to financial loss, theft victims are often left with psychological and emotional scars as a result of these types of crimes. The psychological effects of a break-in can cause burglary victims to feel perpetually unsafe and afraid in even in their own homes. Victims develop a deep distrust of police due to the way break-ins are handled by authorities. As a result of this, many victims even experience difficulties in their careers and personal lives (Siegel, 2008).

2.3 Risk Prevention Techniques

Risk control is an integral part of the risk management process which is a continuous process of identifying, assessing, mitigating, controlling, monitoring and reviewing the risk (Dorfman, 2005). Risk control should add value to any organization (McKinney, 2000). A global security survey conducted by Ernest and Young (2011) found that hospitals that embraced risk control techniques benefitted by cost reduction and value creation thereby improving on their performance. A useful way of categorizing risk control activities is to distinguish activities that alter the frequency of losses from those that alter the severity of loss. Power (2007) puts forward that risk prevention and risk avoidance techniques reduce the frequency of risk while risk retention and risk transfer reduce the severity of risk occurrence. According to Oliver et al (2006) there is a strong correlation between risk control practices and risk reduction. These techniques should also be updated periodically to reflect changes in risks to customers, or to the safety and soundness of the risk programme in hospital.

Theft Risks in hospitals may be reduced, or certainly controlled by using a well-planned loss prevention programme. American institute of safety standards recommends theft prevention techniques in hospitals such as CCTV cameras, security guard, perimeter walls, alarms, burglary proofing. The hospital installs these techniques to reduce either the probability or consequence of the risk (Marshall & Alexander, 2006). The appropriate risk mitigation action varies with the level of risk. This involves selecting one out of four strategies which are



reducing the risk's impact or probability, shifting the risk's timeframe, or changing the risk's consequence, investigation or conducting research until a decision on a mitigation approach can be made, acceptance of the risk by doing nothing with the anticipation that the risk may have to be managed in the future or watching the risk by tracking the risk and its attributes for early warnings signs of critical changes (Preyssl, 1995).

There is usually a trade-off to be made between the magnitude of the risk and the resources needed to reduce that risk to an acceptable level. Detection systems to deter unlawful behavior among employees can serve to a considerable extent in providing close oversight and employee supervision (Sausser, 2007). Originally surveillance cameras systems were installed to deter burglary, terrorism, assault and car theft but their use has been extended to include combating anti-social behavior, such as littering, urinating in public, traffic violations, obstruction, and drunkenness (Buntin, 2008). Marten and Hamman (2002) indicates that surveillance camera can operate 24 hours a day, seven days a week, and 365 days a year without a toilet break, smoke break, or lunch. It does not need a holiday, maternity leave and rarely goes sick .But cautioned that it does not actually do anything. It is the operators that produce the results required. Research has found security strategies, such as the use of security guards and metal detectors to be effective in reducing the frequency of theft in hospitals.

A system of risk reduction metrics should be applied to each plan. Vulnerable or high value materials in hospitals should be subject to tighter controls in terms of its production from storage areas and where staff numbers allow there should be regular patrols through all rooms (Dorfman, 2005).Surveillance equipment such as CCTV can be used to supplement other physical security measures but should not be considered as a substitute for direct staff invigilation. Yellman (2000) recommends that in order to prevent shoplifting, procedures for controlling access to storage areas should be drawn up and strictly enforced and entry limited to personnel with a demonstrable need to gain access. Maintenance staff, cleaners or other external agents should be supervised and procedures established to ensure that their presence in any area does not compromise theft collections. Proofing identity and signing the registers on entering the institution need to be implemented.

Hospital offices and working areas should be designed with good sight lines for staff invigilation and security, avoiding awkward angles, pillars and other obstructions where possible. Money and records can be secured by preventing access to accounts or computer systems, protecting and safeguarding codes and personal identification numbers, use of high quality safes, vaults, and filing cabinets. When facilities are available for the storage of money or valuable equipment, access should be limited to as few people as possible (Tim, 2004). Hospitals may also employ fences to maximize natural surveillance, or the ability to easily keep watch over hospital grounds and monitor the flow of individuals into and out of the campus. The use of physical barriers such as fences and access points such as gates give hospital



planners the ability to distinguish between exclusive and non-exclusive access zones (Fussey, 2010).

2.3.1. Screening and Background Checks

Alison, (2008) recommends that Institutions should always Screen out potential employees and visitors on their histories A full background check can take the form of finger print checks, recommendations from previous employers or authority, requisition of a certificate of good conduct, introductory letters from persons in authority. Universities have an obligation to make sure their work environment is safe for all employees and students.

Background checks are often requested by employers on job candidates for employment screening, especially on candidates seeking a position that requires high security or a position of trust. These checks are often used by employers as a means of objectively evaluating a job candidate's qualifications, character, fitness, and to identify potential hiring risks for safety and security reasons (Pike, 2000).

2.3.2 Metal Detectors

As part of a hospital theft control process, metal detectors provide an added measure of safety when placed in conjunction with well-trained security personnel. Whether a facility uses walk-through metal detectors, handhelds, or, more commonly, both, such devices can provide the foundations for a safe, secure environment where patients and staff can coexist without fear (Mayer, 1999). Random bag checks are extremely effective because a person does not know when he or she will be examined for weapons. Though a portal metal detector grants a hospital a greater degree of certainty as to the presence of metallic objects, conducting random bag checks with handheld metal detectors leads the person to monitor his or her own activity. In short, such unpredictable and unsystematic surveillance actually becomes an omnipresent surveillance in the mind of the person and has the added benefit of saving a hospital both time and money (Mwenda, 2015).

2.3.3 Perimeter Walls

Hospitals may employ fences to maximize natural surveillance, or the ability to easily keep watch over their grounds and monitor the flow of individuals into and out of the compound. Hospitals should ensure that there are no hidden areas on the hospitals grounds, fencing should be placed strategically so as not to obstruct lines of sight (Mwenda, 2015). However, they can mitigate some obstacles to surveillance through appropriate fencing choices. Hospitals can increase visibility by installing openings or windows in solid walls, for instance, or by replacing solid walls with wrought iron fencing. The use of physical barriers such as fences and access points such as gates give school planners the ability to distinguish between exclusive and non-exclusive access zones (Fussey, 2010).



Certain types of fences may provide further safety related benefits. Solid walls or fences, for example, may provide protection against bullets; these types of barriers also may enhance privacy. Short fences, while not effective in controlling access, can help to define ownership of a given territory. Furthermore, such fences can effectively demarcate an area or regulate pedestrian traffic, for instance. Similarly, hostile vegetation dense, thorny groundcover or bushes can be used effectively to define boundaries of various kinds around and within hospital property (Drake, 2008).

2.3.4 Alarms

Alarms are a signal for a hasty emotional response to an emergency. Panic buttons are easily configured to trigger multiple emergency alerts simultaneously such as automatic lockdown procedures, emergency notification, video camera recording and more can all be tied to a panic button. Mobile duress panic buttons are easily integrated into existing hospital security system panels to provide an effective increase in safety of staff and patients. Pressing either a fixed or mobile panic button sends an alert through the existing security system, providing an easy way for anyone to signal for help (Drake, 2008).

While this concept was originally limited to banks and robbery situations, it has seen growth in every sector that interacts with the public such as healthcare, government and education. In fact, nearly every business has a front desk or reception area that requires some form of protection for isolated workers. Therefore, the technology has developed vastly in the past decades from a simple buzzer setting off a signal in a back room, or reaching a call center to notify law enforcement, to complex, multi-level systems that integrate with other security devices. This versatility and adaptation has brought a level of complexity that requires some consideration in its setup and use (Mwenda, 2015).

2.4 Problems Associated with Adoption of Risk Control Techniques

Implementation of the risk management process in hospital programs is not without challenges. Most difficulties may be classified as cultural, or having to do with attitudes and perceptions, rather than with the mechanics of the implementation. First is the inevitable resistance to change. Most people prefer the status quo and resist the introduction of new concepts, processes etc. An attempt that can be made to meet this challenge is by writing a series of memos explaining the process, its purpose, and its implementation as well as making personal contact with the key participants (Elsethet *al.* 1998). Explaining to someone what you are going to do, why, and what benefit it will have for him or her can have a tremendous impact on the other person's attitude toward the process. Another problem can occur during the initial assessment of risk. Some people on a program will react negatively to the connotation of having a risk in their area of responsibility rated as high (Koller, 2000). To overcome this problem a clear template and periodically communicating with the responsible person about the true rating of the risk is necessary. Furthermore it is important to introduce new metrics one at a time, to give people time to assimilate and see the benefits of the new



processes and concepts. In this way you create a certain awareness which leads to not only acceptance of the process, but also active participation in the process.

2.5 Severity and Frequency of Theft Incidents

The international institute of risk management defines severity as the amount of damage that is or that may be inflicted by a loss or catastrophe. Sometimes quantified as a severity rate, which is a ratio relating the amount of loss to values exposed to loss during a specified period.

2.6 Other Factors Influencing Theft in Public Hospitals

Theft in public hospitals is also influenced by other factors which the organizations may not have any influence over. These factors are the Government policies and economic factors.

2.6.1 Government Policies

Public hospitals depend on the government largely when it comes to matter of safety (Buntin, 2008). Presence of armed policemen on public hospitals and in the surrounding areas increases safety and serves as a deterrent to any persons intending to commit theft acts. Government must collaborate with hospitals if safety has to be ensured in the public hospital.

2.6.2 Economic Factors

Risk control techniques require a lot of finances to implement and keep running. The size of a public hospital together with its financial capability and needs will be considered before a hospital implements these techniques. The incomes public hospital generates through various means could be too minimal such that they cannot effectively install these techniques.

2.7 Empirical Review

According to McKinney (2000), risk control measures are widely used to reduce occurrence of risks affecting maximization of profits. He further found that risk management techniques, when applied properly e.g. risk transfer and sharing, risk avoidance and risk prevention could be used to reduce impact of loss. McKinney recommends that every organization should have a good risk management plan that contains a schedule for control implementation and responsible persons for those actions.

Peshawar(2014) on his study on hospital theft notes that one of the most common problems explored in the literature relating to issues with hospital theft is the fact that many threatening incidents go unreported. He recommends that continuous security training is a solution since people know who to report to and are able to detect any suspicious activities. This is especially troublesome because many hospital administrators base their policies and techniques on the types of crimes and threatening incidents that are reported.

Bowers *et al.* (1998) notes that Health care facilities are likely to have very high theft risk rates. Hospitals are more exposed to the risk of theft due to large and diverse population of



people they control. He notes the threat of theft can be from the employees or the external environment. He points out that once a theft has occurred there is little chance of catching the offenders or recovering stolen property because majority of thieves dress as hospital workers or Service Company employees and get away with expensive medical equipment and valuable properties from the hospitals.

Ernest and Young (2011) found that the firms with mature risk management practices benefitted by early identification of risk and mitigation, cost reduction and value creation thereby improving on business performance. Their survey further found that Institution performance was highly correlated with the level of integration and coordination across risk, control and compliance function.

2.9 Theoretical framework

The study is grounded on three theories; Homeostasis, Resilience and Routine activity. Homeostasis theory maintains that, in any activity, people accept a certain level of subjectively estimated risk to their health, safety, and other things they value, in exchange for the benefits they hope to receive from that activity. In other words, individuals adjust their level of risk-taking behavior depending on the safety measures that are in place. In any ongoing activity, people continuously check the amount of risk they feel they are exposed to. They compare this with the amount of risk they are willing to accept, and try to reduce any difference between the two to zero. Thus, if the level of subjectively experienced risk is lower than is felt acceptable, people tend to engage in actions that increase their exposure to risk. If, however, the level of subjectively experienced risk is higher than is acceptable, they make an attempt to exercise greater caution(Wilde, 2014).

Resilience theory also has a direct relationship with this study. In general the presence of one or more protective factors should reduce the effects of exposure to adversity. The more protective factors are available, the more resilient institutions are to risk (Resnick,2000).In the context of hospital set ups protective techniques like the security guards, surveillance system, Perimeter walls and fences are supposed to reduce the severity and the frequency of theft. With risk prevention, theft in hospital should be very low or even reduced to zero as the techniques should help the institution resist any attempt of theft.

Routine activity theory, developed by Marcus Felson and Lawrence Cohen is linked to this study because it puts forth that theft depends on the opportunities available. If a target is not protected enough, and if it is worth the reward, theft will happen, it just needs an opportunity (Guly, 2004). Hospitals are highly vulnerable to theft risk posed by the many opportunities available including huge numbers of medicine received in the hospital by people who themselves own chemists and pharmacies, valuable properties owned by sick helpless patients, or even the hospital staff who are entrusted with the hospital resources.

3. METHODOLOGY

3.1 Research Design

This study employed a descriptive research design that described the state of affairs at the time of data collection. It involved assessing attitudes or opinions and thoughts about effectiveness of risk prevention techniques on theft severity and frequency. The research design was able to reveal and measure the strength of the target group's opinion, attitude, and behavior with regards to theft in hospitals.

3.2 Location of the Study

This study was carried out in Embu County which is on the eastern slopes of Mount Kenya. The choice of Embu County Public hospitals is inferred from the 2014 ministry of health report that named Embu level five hospital among the hospitals with highest number of reported theft cases. The choice of Embu County was also because it was easily accessible to the researcher was able to create a rapport with the respondents. An ideal location of any study should be easily accessible to the researcher and should be that which permits rapport with the informants (Singleton, 2003).

3.3 Population of the Study

All items of interest in an inquiry constitute a population (Kothari, 2004). This study targeted a population of 1608 hospital staff from all the five public hospitals in Embu county.

Table 1: Population of Study

Description	Senior Staff	Junior Staff
Kianjokoma Sub District Hospital	7	251
Mbeere District Hospital	9	202
Ishara Sub District Hospital	6	231
Runyenjes District Hospital	13	280
Embu General Hospital	21	588
Total	56	1552

Source: Profiles of the Public Hospitals (2015)

3.4 Sampling Procedure and Sample Size

This research stratified the population into junior staff and senior staff. Senior staffs were picked through a census and junior staffs through a simple random sampling. Simple random sampling was preferred because it gives each subject an equal chance of taking part in the study (Calmorin, 2007). The simple random sampling was necessitated by guidelines given by Nasiuma (2001).



$$n = \frac{NC^2}{C^2 + (N-1)e^2}$$

Where n=population

c=coefficient of variation which is <30%

e=standard error which is fixed between 2-5%

Taking a coefficient of variation of 26.8% and a standard error of 0.02 out of a target population of 1552 hospital staffs, a sample of 161 will be obtained.

The senior staffs are charged with making decisions on implementation of risk prevention techniques. The advantage of employing a simple census is accuracy since the whole population is counted and in detail also reliable statistics about the whole population obtained (Kathuri and Pals, 1993). The management staff was relatively small; hence it necessitated the researcher to use this method to enhance reliability of information to be collected.

Table 2: Sample size

Description	Senior Staff	Junior Staff
Kianjokoma Sub District Hospital	7	26
Mbeere District Hospital	9	21
Ishara Sub District Hospital	6	24
Runyenjes District Hospital	13	29
Embu General Hospital	21	61
Total	56	161

3.6 Data Collection

Primary data was obtained from the hospital staff through use of questionnaire. Questionnaires were preferable because they enable the researcher to establish rapport with the respondents while at the same time get accurate information. This also eases the standardization of responses and solicits for similar information from the respondents capturing both dependent and the independent variables (Mertens, 2005).

3.7 Data Analysis and Presentation

Data was cleaned by being checked for logical consistency and any unnecessary data removed. It was then refined and processed using statistical package for social sciences (SPSS) version 23. Martin and Acuna (2002) observe that, SPSS is able to handle large amount of data given its wide spectrum of statistical procedures purposefully designed for social sciences, it is also quite efficient. Quantitative analysis that entailed analyzing numbers about a situation by choosing specific aspects of that situation was used. The results of data analysis have been presented in frequency tables and percentages. Chi-square test was used to show the



association between variables and test hypothesis. A 5% level of significance was considered. Table 3 gives a summary of the methods for data analysis.

Table 3: Data Analysis Matrix

Research Hypothesis	Independent Variable	Dependent Variable	Statistical Tools
H₀₁ Risk prevention techniques have no significant association with theft in public hospitals	Risk Prevention techniques	Theft in public Hospitals	Percentages Chi-square test Frequencies

4. RESULTS AND DISCUSSIONS

4.1 Response Rate

According to Mugenda and Mugenda (2003) 100% response rate is unlikely. The sample needs to be larger enough to ensure sufficient response for the required margin of error. For this study a total of 217 questionnaires were distributed to the respondents. The response rate is as shown in table 4

Table 4: Hospital staff response rate

Description	Senior staff	Junior staff
Frequency %		Frequency %
Kianjokoma Sub District Hospital	610.71	25 15.52
Mbeere District Hospital	712.5	20 12.42
Ishiara Sub District Hospital	610.71	20 12.44
Runyenjes District Hospital	1323.21	27 16.77
Embu Provincial General Hospital	1933.93	56 34.78
Un answered questionnaire	58.93	138.07
Total	56100	161 100

This study issued 56 questionnaires targeting the senior staff and 161 questionnaires targeting junior staffs. From table 4, 91.93% of junior staff and 91.07% senior staff responded. According to Mugenda and Mugenda (2003) a return of 50% and above of the research instruments is acceptable.

4.2 Adoption of Risk prevention Techniques by Public Hospitals

The risk prevention techniques in a hospital are responsible for protection against all manner of risk through reducing the risk frequency and its severity if it occurs. Thus, they are responsible for ensuring a safe environment to the hospital and the people. This study sought to find out the risk prevention techniques adopted by public hospitals in Embu County. The results were presented in table 5.



This study sought to find out from the junior staff whether hospitals had adopted risk prevention techniques and the findings were presented in table 8. These findings were similar with those of the senior staff as majority (51.4%) CCTV cameras, (56.8%) screening and background checks, (60.1%) metal detectors and (51.4%) perimeter walls indicated that public hospitals had fully adopted risk prevention techniques. The least employed prevention technique was intelligence services rated to be partially adopted by a majority 41.2%.

From these results it can be concluded that risk prevention techniques adopted by the hospitals vary and are not adopted at similar levels thus protection of people and hospital property from theft is not guaranteed. According to Mwenda (2015), the frequency and severity of risk incidents is greatly increased when there is lax in adoption and implementation of risk prevention techniques. He therefore recommends that full adoption must be done at all levels to ensure protection for all individuals and property in a hospital. Richards (2013) also notes that for an institution to be free of theft, risk control techniques have to be adopted at similar level. Public hospitals should therefore consider fully adopting the risk control techniques.

Table 5: Adoption of Risk Preventions Techniques

4.3 Employment of Risk Prevention Techniques by Public Hospitals

The possibility and outcome of any theft incident is highly dependent on the nature of risk

Adoption of Risk Prevention Technique	Fully adopted		Partially adopted		Not Adopted		Mean	Standard deviation
	F	%	F	%	F	%		
CCTV cameras	30	58.8	11	21.6	10	19.6	1.6078	.8019
Screening and background checks	42	82.4	6	11.8	3	5.9	1.2353	.5509
Intelligence services	15	29.4	26	51.0	10	19.6	2.0980	.7001
Theft audits	20	39.2	16	31.4	15	32.4	2.0980	.8307
Metal detectors	38	74.5	10	19.6	3	5.9	1.3137	.5827
Perimeter walls	35	68.6	11	21.6	5	9.8	1.4118	.6686
Panic buttons	16	31.4	21	41.2	14	27.5	2.0392	.7735

control techniques present in a hospital. The 2004 edition of American national standards report indicates that effective employment of risk prevention techniques will address the protection, mitigation, preparedness, response and recovery from theft incidents. This study therefore sought to find out the level of employment of risk prevention techniques by public hospitals. Data gathered was analysed using percentages and the results presented in closed tabulations by table 6 for junior staff and table 7 for senior staff.



Table 6: JuniorStaff Response on level of Employment of Risk Prevention Techniques

Employment of risk Prevention techniques	Very Low	low	Moderate high	high	very mean deviation	standard
	%	%	%	%	%	
CCTV cameras	12.2	23.0	41.9	12.2	10.8	2.8649 1.1227
Screening and background checks	16.2	27.0	28.4	20.3	8.1	2.7703 1.1843
Intelligence services	27.0	21.6	25.7	19.6	6.1	2.5608 1.2466
Theft audits	14.9	21.6	32.4	21.6	9.5	2.8919 1.1845
Metal detectors	10.8	23.0	29.7	20.3	16.2	3.0811 1.2314
Perimeter walls	8.1	24.3	31.8	16.2	19.6	3.1486 1.2253
Panic buttons	44.6	32.4	12.2	8.1	2.7	1.9189 1.0659

From the junior staff responses presented in table 9 it emerged that most public hospitals had not fully employed risk control techniques. Majority of junior staff(41.9%) CCTVcameras,(29.7%) metal detectors,(31.8%) perimeter wall and (28.4%)screening and background checks indicated that risk prevention techniques were moderately employed. Panic buttons were rated to be the least employed with majority (44.6%) indicating low employment.

These results show that public hospitals are vulnerable to theft due to the low employment level of risk prevention techniques by the public hospitals. Gully (2004) notes that if a target is not protected enough, and if it is worth the reward, theft will happen, it just requires an opportunity. Therefore public hospitals should improve on their level of risk prevention techniques employment to ensure adequate protection. Resnick(2000) recommends that the more protective factors public hospitals will effectively employ, the more resilient hospitals will be torisk of theft.



Table 7: Senior Staff Response on Level of Employment of Risk Control Techniques

Employment of risk control techniques	Very Low	low	moderate	high	very high	mean	standard deviation
	%	%	%	%	%		
CCTV cameras	17.6	19.6	33.3	19.6	9.8	2.8431	1.2226
Screening and background checks	5.9	11.8	39.2	19.6	23.5	3.4314	1.1533
Intelligence services	11.8	23.5	47.1	11.8	5.9	2.7647	1.0117
Theft audits	11.8	21.6	25.5	23.5	17.6	3.1373	1.2809
Metal detectors	2.0	5.9	21.6	31.4	39.2	4.0000	1.0198
Perimeter walls	2.0	3.9	43.1	31.4	19.6	3.6275	.9156
Panic buttons	27.5	35.3	19.6	15.7	2.0	2.2941	1.1008

Table 7 presents results from senior staff regarding the level of employment of risk prevention techniques. From these results, the highest percentage of the senior staff indicated that risk control techniques were moderately employed. This was indicated by (33.3%) CCTV cameras, (47.1%) intelligence services, (43.1%) perimeter walls and (39.2%) screening and backgrounds checks who indicated risk prevention techniques were moderately employed. The senior staff responses were similar to those of the junior staff thus it was concluded that even though public hospitals had employed risk prevention techniques there was still a high probability of theft occurring and resulting to severe losses. All the public hospitals should therefore ensure adequate and full employment of risk prevention techniques in order to guarantee a theft free environment.

4.4 Effectiveness of Risk Prevention Techniques

Young (2014) in his research on security risk noted that most organizations including hospitals already have risk prevention, risk retention and risk transfer techniques that aim to minimize the destruction of property and loss of life. However, these risk prevention techniques can be in an organization but also may not be effective. It’s for this reason that this study sought to find the effectiveness of risk control techniques in reducing theft frequency and severity. Descriptive statistics of frequencies and percentages were used to analyse the data collected and the results presented in tables 8 for senior staff and table 9 for junior staffs.



Table 8: Senior Staff Response on Effectiveness of Risk Prevention Techniques

Effectiveness of risk prevention techniques	Very effective		Fairly effective		Not effective		Mean	Standard deviation
	F	%	F	%	F	%		
CCTV cameras	13	25.5	28	54.9	10	19.6	1.9412	.6756
Screening and background checks	16	31.4	23	45.1	12	23.5	1.9216	.7441
Intelligence services	8	15.7	36	70.6	7	13.7	1.9804	.5473
Theft audits	18	35.3	26	51.0	7	13.7	1.7843	.6727
Perimeter walls	26	51.0	19	37.3	6	11.8	1.6078	.6950
Metal detectors	12	23.5	28	54.9	11	21.6	1.9804	.6779
Panic buttons	14	27.5	18	35.3	19	37.3	2.0980	.8063

According to the senior staff results in table 11, majority (54.9%) CCTV cameras, (45.1%) screening and background checks, (70.6%) intelligence services and (54.9%) metal detectors rated risk prevention techniques to be fairly effective. It's worth noting that majority (51.0%) considered perimeter walls to be the most effective risk prevention technique.

Responses from the senior staffs were considered to be more reliable. Wilde (2014) in his homeostasis theory maintains that people accept a certain level of subjectively estimated risk to their health, safety and other things they value, in exchange to the benefit they hope to receive from that activity. They compare this with the amount of risk they are willing to accept, and try to reduce any difference between the two to zero. He further notes that if the level of subjectively experienced risk is higher than is acceptable, people make an attempt to exercise greater caution. In other words, individuals adjust their level of risk-taking behavior depending on the safety measures that are in place.

Table 9: Junior Staff Response on Effectiveness of Risk Prevention Techniques

Effectiveness of risk prevention technique	very effective		Fairly effective		Not effective		Mean	Standard deviation
	F	%	F	%	F	%		
CCTV cameras	20	13.5	116	78.4	12	8.1	1.9459	.4634
Screening and background checks	10	6.8	84	56.8	54	36.5	2.2973	.5885
Intelligence services	15	10.1	57	38.5	76	51.4	2.4122	.6696
Theft audits	32	21.6	80	54.1	36	24.3	2.0270	.6796
Metal detectors	36	24.3	62	41.9	50	33.8	2.2703	.8131
Perimeter walls	62	41.9	50	33.8	36	24.3	2.1757	.7972
Panic buttons	34	23.0	74	50.0	40	27.0	2.3108	.7545



Table 9 presents results from junior staff on level of effectiveness of risk control in reducing theft in public hospitals. From this table majority (78.4%) CCTV cameras, (56.8%) screening and background checks and (54.1%) theft audits rated risk prevention techniques to be fairly effective in reducing theft frequency. Findings from the junior staff were similar when compared to those of senior staff indicating public hospitals need to review their implementation levels if effectiveness of risk prevention techniques has to be improved. The healthcare international association for safety and security (2014) recommends that frequency and severity of theft incidents can be controlled to minimum levels by constantly monitoring and evaluating the risk control techniques put in place.

4.5 Frequency of Theft Incidents in Public Hospitals

Richards (2014) explains theft frequency as the rate at which theft may or may not happen. Theft frequency is a conclusive measure of how effective risk prevention techniques are in achieving their set objectives. When theft frequency is high, risk prevention techniques are considered not effective and vice versa is true. This study therefore sought to find out how frequent theft occurred in the public hospitals. Descriptive statistics of frequencies and percentages were used to analyse the data and the results presented in table 10 for senior staff and table 14 for junior staff.

Table 10: Senior Staff Responses on Theft Frequency in Public Hospitals

Theft frequency	very frequent		Frequent		once in a while		Never		Mean	Standard deviation
	F	%	F	%	F	%	F	%		
Burglary	3	5.9	17	33.3	30	58.8	1	2.0	2.5686	.6404
Larceny	12	23.5	7	13.7	21	41.2	11	21.6	2.6078	1.0780
Shoplifting	24	47.1	16	31.4	8	15.7	3	5.9	2.4314	.8307
Medical identity theft	8	15.7	18	35.3	24	47.1	1	2.0	2.3529	.7700
Robbery	11	21.6	16	31.4	18	35.3	6	11.8	2.0980	1.0247

Table 10 presents findings obtained from senior staffs on frequency of theft in the public hospitals. The results revealed that theft frequency was low and occurred once in a while. This was indicated by majority of the senior staff (58.8%) burglary, (41.2%) larceny, (35.3%) robbery and (47.1%) medical identity theft indicating theft occurred once in a while. Shoplifting was the most frequent theft incidents with majority 47.1% rating it as very frequent. Most of the senior staff attached occasional medicine losses to shoplifting. The low rate of theft frequency was attributed to public hospitals adopting most of risk prevention techniques



Table 11: JuniorStaff Response on Theft Frequency in Public Hospital

Theft Frequency	very frequent		Frequent		once in a while		never		Mean	standard deviation
	F	%	F	%	F	%	F	%		
Burglary	19	12.8	53	35.8	71	48.0	5	3.4	2.4189	.7560
Larceny	19	12.8	40	27.0	83	56.1	6	4.1	2.5135	.7691
Shoplifting	97	65.5	32	21.6	8	5.4	11	7.4	2.7500	.6687
medical identity theft	26	17.6	30	20.3	89	60.1	3	2.0	2.4662	.8031
Robbery	17	11.5	32	21.6	94	65.3	5	3.4	2.5878	.7370

Findings from junior staff on theft frequency in public hospitals were presented in table 11. From these findings, majority 66.2% indicated that shoplifting was very frequent while burglary (48.0%), larceny (56.1%), medical identity theft (60.1%) and robbery (65.3%) occurred once in a while. These results are consistent with those of the junior staff hence a true reflection of theft frequency in the public hospitals. This results were also in line with resilience theory that puts forth that presence of one or more protective factors should reduce the effects of exposure to adversity. The more protective factors are available the more resilient institutions are to risk (Resnick, 2000).

4.6Severityof Theft in Public Hospitals

Most public hospitals learn how to respond to theft incidents only after suffering severe attacks that result to significant losses. Risk retention and risk transfer techniques are meant to reduce severity of losses. When theft severity is high, risk retention and transfer techniques are considered not effective and vice versa are true. This study therefore sought to determine the severity of theft incidents in public hospitals. Descriptive statistics of frequencies and percentages were used to analyse the data and results presented in table 12 for senior staff and table 13 for junior staff.



Table 12: Senior Staff Responses on Theft Severity in Public Hospital

Theft Severity	very severe		Severe		not severe		No incident		Mean	Standard deviation
	F	%	F	%	F	%	F	%		
Burglary	12	23.5	24	47.1	10	19.6	5	9.8	1.9216	1.0362
Larceny	18	35.3	19	37.1	11	21.6	3	5.9	2.2549	.8681
Shoplifting	3	5.9	20	39.2	26	51.0	2	3.9	1.6275	.7735
Medical identity theft	18	25.3	22	43.1	10	19.6	1	2.0	1.8824	.7911
Robbery	12	23.5	28	54.9	8	15.7	3	5.9	1.7255	.9397

From the findings in table 15, theft severity in public hospitals was rated to be highly severe. This is because most of the senior staff (47.1%) burglary,(37.1%) larceny,(43.1%) medical identity theft and robbery (54.9%) indicated that when theft occurred it resulted to severe losses. Severity of shoplifting was classified notsevere by a majority 51.0%.

Table 13: Junior Staff Response on Theft Severity in Public Hospitals

Theft severity	very severe		Severe		not severe		no incident		Mean	Standard deviation
	F	%	F	%	F	%	F	%		
Burglary	56	37.8	64	43.2	23	15.5	5	3.4	1.7905	.82687
Larceny	24	16.2	88	59.5	30	20.3	6	4.1	1.6892	.93205
Shoplifting	28	18.9	36	24.3	74	50.0	10	6.8	2.4459	.87508
Medical identity theft	48	32.4	74	50.0	23	15.5	3	2.0	1.8716	.74029
Robbery	33	22.3	99	66.9	15	10.1	1	.7	1.4459	.70261

Results presented in table 16 shows that majority of the junior staff (43.2%) burglary,(59.5%)larceny,(50.0%) medical identity theft and (66.9%) robbery indicated that theft incidents were severe when they occurred. Half of the junior staff (50.0%) indicated that shoplifting incidences were not severe. These results were similar with those of the senior staffs. This implied that risk transfer and risk retention were not effective in reducing theft severity in public hospitals. Public hospitals should therefore focus on employment levels of these techniques if they are to be effective in reducing theft severity. These results on theft frequency and severity were consistent with Henrichtriangle that puts forth if the frequency of theft incident is high, the severity is low and vice versa is true (Dorfman, 2005).



4.7 Effect of Risk Prevention Techniques on Theft in Public Hospitals

Routine activity theory developed by Marcus Felson and Lawrence Cohen puts forth that theft depends on the opportunities available (Gully, 2004). The choice of a theft target is highly dependent on the perceived effectiveness of risk control techniques in the hospital. This study therefore sought to establish the effect of risk control techniques on theft in public hospitals. This was facilitated by establishing the association of risk prevention, transfer and retention techniques with theft in the public hospital. These results were further tested for significance using chi-square test at a 5% level of significance.

4.7.1 Association of Risk Prevention Techniques with Theft in Public Hospitals

Prevention techniques are designed to reduce theft frequency by detecting theft before they happen and deterring people from committing such incidents. This study sought to establish the association of prevention techniques with theft frequency in public hospitals. To measure the association of prevention techniques with theft frequency in public hospitals a prevention technique index (PTI) was computed. The index consisted of seven variables representing seven risk prevention technique employed by the public hospitals. These prevention techniques were CCTV cameras, screening and background checks, Intelligence services, safety audits, perimeter walls, metal detectors and panic buttons. The variables were scored on a likert scale of 1-4 with 4 representing the highest scores implying theft has never occurred and 1 representing the lowest score meaning theft occurs very frequently.

$$PTI = \frac{CCTV + SBC + IS + SA + PM + MD + PB}{7}$$

Where CCTV=closed circuit television video, SBCP=screening and background checks, IS=intelligence services, SA=safety audit, PM=Perimeter walls, MD=Metal detectors, PB=Panic buttons. The results were the presented in Table 14.

Table 14: Association of Risk Prevention Techniques with Theft Frequency in Public Hospitals

Effectiveness of Risk Prevention Techniques	Theft Frequency				
	Very frequent	Frequent	once in a while	Never	Totals
Not sure	0%	0.50%	0.50%	0%	1.00%
Not effective	1.00%	18.09%	10.05%	0%	29.15%
Moderate effectives	0%	19.09%	33.67%	0%	52.76%
Effectives	0%	5.03%	11.55%	0%	16.58%
Very effectives	0%	0%	0.50%	0%	0.50%
	1.00%	42.71%	56.28%	0%	100%

Chi-square=20.00, df=12, p-value=0.046

Results on table 14 revealed that majority (69.84%) indicated that risk prevention techniques were effective in preventing theft. Among those who indicated prevention techniques were



effective in reducing theft frequency, 33.67% indicated that theft occurred once in a while when prevention techniques are moderately effective. 11.55% of those who indicated risk prevention techniques were effective in reducing theft also indicated that theft occurred once in a while. Only 29.15% of the total respondents indicated that risk prevention techniques were not effective while a majority (56.28%) indicated that theft frequency was very low with incidents happening once in a while. Majority of the respondents who indicated that risk prevention techniques were effective also rated theft frequency to be low in public hospitals.

These results were further tested for significance using chi-square test at 5% significance level. The computed chi-square value was 20.000 and a p-value=0.046 was obtained therefore concluding that there was a significant association of risk prevention technique with theft frequency in public hospitals in Embu county. This study thus rejected the null hypothesis (H_{01}) which stated that risk prevention techniques had no significant association with theft in public hospitals in Embu County.

The implication of these findings was that risk prevention techniques were effective in reducing theft frequency in public hospitals in Embu County. These results were consistent with (Resnick, 2000) findings that the more protective factors are available, the more resilient hospitals will be to theft and that the presence of preventive techniques like perimeter walls, surveillance systems and metal detectors reduce the frequency of theft.

5. SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.1 Summary of the Findings

This study evaluated the effect of risk prevention techniques on theft in public hospitals in Embu County.

This study found out that public hospitals had adopted various risk prevention techniques which were CCTV cameras, metal detectors, intelligence services, screening and background checks, theft audits, perimeter walls and panic buttons. This study further found out that prevention techniques were employed at different levels with majority being moderately employed. It was also established that prevention techniques were fairly effective in reducing theft frequency in public hospitals. Overall results revealed that risk prevention techniques had a significant association with theft in public hospitals with chi-square value of 20.00 and a p-value of $0.046 < 0.05$ at a 5% level of significance.

Results on theft frequency and severity revealed that most of the public hospitals at some point had experienced a theft incident. Theft frequency was low with robbery, burglary, larceny and medical identity occurring once in a while. The findings further revealed that theft severity in the public hospitals was high with larceny being very severe. Shoplifting was the least severe of the theft incidents reported.



5.2 Conclusion

Based on the findings of this study the following conclusions were made:

Risk prevention techniques had a significant association with theft in public hospitals therefore the null hypothesis that risk prevention techniques have no significant association with theft in public hospitals was rejected at a 5% level of significant. It was therefore concluded that public hospitals in Embu County had adopted and fairly employed risk prevention techniques that resulted to the low theft frequency.

5.3 Recommendations

From the findings of this study, the following recommendations were made:

- i. Public hospitals should continuously monitor and evaluate risk prevention techniques so that any defective technique is replaced therefore maintaining the low levels of theft frequency.
- ii. Public hospitals should consider adopting and fully employing risk transfer techniques among them insurance, leasing and hold harmless agreements in order to transfer theft risks to a third party therefore reducing theft severity when it occurs.
- iii. Public hospitals should also adopt and fully employ risk retention techniques like captives, borrowing, current expensing and maintaining reserves thus minor losses resulting from theft can be borne by the hospitals without having to interrupt the daily activities. This will therefore reduce the severity of theft in the public hospitals.

REFERENCES

- Alison, W. (2008). *The July 2005 Bombings*. Paper presented at the Local Government Agency 2007 CCTV Conference: The Development of a National Strategy, Innovative Systems, Effectiveness and Standards, Local Government House, London.
- Biegelman, Martin T. (2013). "Unhealthy Procedures: Medical Identity Theft." *association of Certified Fraud Examiners*.
- Bowers, K., Hirschfield, A., & Johnson, S. (1998). Victimization revisited: A Case study of non-residential repeat burglary on Merseyside. *British Journal of Criminology*, 39, 429-452.
- Buntin, J. (2008). Security Preparations for the 1996 Centennial Olympic Games. *Cambridge, MA: John F. Kennedy School of Government, Harvard University*.
- Cardwell, M., & Cardwell, M. (1999). *Complete AZ psychological handbook*: London: Hodder and Stoughton Educational.



Crocker, K. J. and Tennyson, S., 1999, Costly state falsification or verification? Theory and evidence from bodily injury liability claims, in: C. Laberge-Nadeau and

G. Dionne, eds. *Automobile Insurance: Road Safety, New Drivers, Risks, Insurance Fraud and Regulation* (Boston, Mass.: Kluwer).

Cromwell, P., & Olson, J.N. (2006). The reasoning burglar: Motives and decision-making strategies. In P. Cromwell (Ed.), *In their own words: Criminals on Crime* (4th ed.). (pp.42-54). Los Angeles, CA: Roxbury.

Dimkov, T. W. Pieters, and P. Hartel. *Two methodologies for physical penetration testing using social engineering*. Technical report, CTIT, December 2009.

Dorfman, M.S. (2005) *Introduction to Risk Management and Insurance* (8th edn). Asoke K. Ghosh. MUMBAI

Elseth, B.O. and Hamann, R.J. (1998). *The evaluation Of Risk Management Tools, Proceedings 15th Int. Cost Engineering Congress*.

Ernst & Young. (2011). *Global information security survey*. Ernst & Young.

Fischer, R. J. & Green, G. (2004). *Introduction to security*. (7th ed.). Boston: Butterworth Heinemann.

Fussey, P. (2010). *Securing and sustaining the Olympic City: reconfiguring London for 2012 and beyond*: Ashgate.

Gallardo, J. (1997). *Leasing to support small businesses and microenterprises*. In: The World Bank. Policy Research Working Paper 1857. December 1997.

Harrington, Scott .E. and Niehaus, Gregory .R. (2004). *Risk management and Insurance .new del.*

Healthcare Information and Management Systems Society (2012). Analytics Report: *Security of Patient Data*.

Healthcare Information and Management Systems Society (2014) *Creating a Trusted Environment; Reducing the Threat of Medical Identity Theft*.

Hubbard, Douglas (2009). *The Failure of Risk Management: Why It's Broken and How to Fix It*. John Wiley & Sons. p. 46.



Human Security Report (2014): Republic of Kenya.

Kallman, J. 2009. *The 2009 Supplement to The Tools & Techniques of Risk Management*

Kathuri, N. J., & Pals, D. A. (1993). *Introduction to educational research*. Educational Media Centre. Egerton University.

Kimama, F.M. (2011). *Risk factors affecting hospital performance in Kenya*. Retrieved from erpository.uonbi.ac.ke

Kothari, C. (2004). *Research Methodology: Methods and Techniques* (2nd ed.). New Delhi: Age International (p) Ltd

Kombo, D.K. & Tromp, L.A. (2006). *proposal and thesis writing: An introduction*. Nairobi: Pauline publications Africa.

Koller, G. (2000). *Risk modeling for determining value and decision making*. Boca Raton: Chapman and Hall/CRC.

Lindstrom, P. (1997). Patterns of school crime: A Replication and empirical extension. *British Journal of Criminology*, 37, 121-130.

Knafla A. Louis (2003). *Crime, Punishment and Reform in Europe*. Greenwood Publishing Group. p. 17. ISBN 0313310149.

Maarten G.H. Bijl and Robbert J. Hamann (2002) *Risk Management Literature Survey; An overview of the process, tools used and their outcomes*; Delft University of Technology.

Marshall, M. I., & Alexander, C. (2006). Using a contingency plan to combat human resource risk" *Journal of Extension* [On-line], 44(2) Article 21AW 1. Available at: <http://www.joe.org/joe/2006april/iw1.shtml>

Mawby, R. (2006). Commercial burglary. In M. Gill (Ed.), *The Handbook of security* (pp. 281-301). Basingstoke, UK: Palgrave Macmillan.

Mayer, J. D. (1997). Artificial intelligence and the identification of emotion. *Intelligence*, 22(2), 89-113.

McKinney, D. (2000). Risk Reduction Through Changing Success Criteria, Proceedings INCOSE International Symposium 2000,



Mertens, D. M. (2005). *Research in education and psychology: Integrating diversity with quantitative, qualitative and mixed methods*. Thousand Oaks, CA: Sage.

Ministry of Health.(2014). *Kenya health assessment system*. Nairobi: United States Agency for International Development.

Ministry of Health.(2014). *Kenya Health Policy 2014-2030*. Nairobi.

Mugenda, O.M., &Mugenda, A.G. (2003). *Research Methods Quantitative and Qualitative Approaches*. Nairobi: Acts Press

Mugenda , O. &Mugenda A. (2008). *Research methods. Quantitative and Qualitative approaches*. Kenya, Nairobi: Act press.

Mulusa, T. (2008). *Evaluating Education Research for Beginners'*: A Practical Study Guide, Nairobi University press, Kenya.

Mwenda,T. M (2015) *effects of security control programmes on safety in universities in Tharaka Nithi and Meru County*(unpublished M.B.A Proposal.Chuka University.)

Nassiuma, D. K. (2000). *Survey sampling: Theory and methods*.

Nyongesa H, C.(2015). *Perceptions of medical students towards healthcare devolution: an online cross-sectional study*. The Pan African medical journal.

Ochieng.p.(2014). *safety and security in Kenyan universities.Recent dynamics in securing students*.

Oliver, Barbara B. and Heather Knight, (2006); *"Introduction to Risk Management" in Public Sector Risk Management*; Public Risk Management Association.

Orodho, J. (2013). *Techniques of writing research proposals and reports in education and social sciences*. Nairobi: Masola Publishers.

Peshawar, N. (2014). *Management of Security: sources, methods, and channels*. *Insecurity and Political Violence*, 15(4), 59-82.

Power M.2007. *Organized Uncertainty: Designing a World of Risk Management*. Oxford:Oxford University Press.



- Preyssl, C (1995). *Safety risk assessment and management - The ESA approach* Reliability Engineering and System Safety # 49 1995
- Rejda, George E .(2001)*Principles of Risk Management and Insurance (11th Ed.)*., Addison Wesley publishers, Boston, Mass.
- Rengert, G.F., &Wasilchick, J. (2000).*Suburban burglary: A tale of two suburbs* (2nd ed.).Springfield, IL: Charles C. Thomas Publisher, Ltd
- Resnick, M. (2000). "Protective Factors, Resiliency, and Healthy Youth Development, Philadelphia, Hanley &Belfus, Inc." Adolescent Medicine: State of the Art Reviews Vol.II (No.1, February).
- Richards, A. (2014). The problem with 'radicalization': the remit of 'Prevent'and the need to refocus on terrorism in the UK. *International Affairs*, 87(1), 143-152.
- Sagimo ,O.p(2013).management dynamics: *Towards efficiency,effectiveness,competence and productivity*.Nairobi,Kenya:east African educational publishers
- Sausser,W.(2007). Employee Theft: Who, How, Why, and What Can Be Done. *SAM Advanced Management Journal* , 72 (3), 13-25.
- Sennewald, Charles A(1992). *Shoplifting*. Boston: Butterworth-Heinemann.
- Serakan, H. (2006). Qualitative research in OM: Criteria for evaluation.
- Siegel, L.J. (2008) "*Criminology*," Belmont, Calif.: West/Wadsworth Publishing Companyhi.lil publishing company limited.
- Singleton, R. (2003). *Approaches to social research*: Oxford University Press.
- Tim prenzler.(2004). *Preventing burglary in commercial and institution settings*, a place ,management and partnership approach. United States of America.
- Vander.Belan,T.(2014).*The Kenyan pharmaceutical sector and crime vulnerabilities*.Antwerp:maklu publishers.
- Wilde, G.J.S. (2014).Target risk: *Dealing with the danger of death, disease and damage in everyday decisions*. Toronto, Canada: PDE Publications.



Wright, R.T., & Decker, S.H. (2014). *Burglars on the job: Street life and residential break-ins*. Boston: Northeastern University Press.

Yellman, T.W. (2000). *Three Facets of Risk*, Proceedings 2000 World Aviation

Young, R. (2014). Defining security risk: The Evolution of Insecurity, control, Its Influence on Definitions in Domestic Legislation-united states. *BC Int'l & Comp. L. Rev.*, 29, 2