American Journal of Humanities and Social Sciences Research (AJHSSR)
e-ISSN :2378-703X
Volume-3, Issue-4, pp-01-13
www.ajhssr.com
Research Paper Open Access

Complacency and Security Management Practices in Nairobi City County, Kenya

Cosmas Ekwom Kamais[1]

[1]*Department of Peace Security and Social Sciences, Egerton University, Nakuru, Kenya*.

ABSTRACT : Human beings are known to have heightened alertness when there is an impending security risk, during an attack or shortly after an attack. It is a confounding phenomenon since it seems to be the norm and also it has not received much investigative scholarly attention. Unfortunately, this kind of behaviour further reverses security mitigation measures that have been instituted and facilitates in further creating insecure environments. The study found that complacency leads to a high likelihood of security lapses/ breaches as confirmed by 45% of the respondents. The also study established that among possible measures to reduce instances of complacency in security management, administrative discipline, reduced working hours in a shift, transfers, prosecution of security managers for negligence and training ranked higher with 78%, 72%, 68%, 64% and 54% respectively. The study recommends empirical research to be done to gain understanding of complacency in security management practices.

KEYWORDS:*Al – Shabaab, As Low as Reasonably Practicable, Explosives, Global War on Terror, Grenades, Complacency, Security Managers, Terror attack.*

I. INTRODUCTION

Kenya has become one of the main partners in the Global War on Terror (GWOT) after the September 2001terror attack in the USA. Kenya is an ally to the US and the nation had to endure various terror incidents in the past few decades. The American embassies in Tanzania and Kenya were attacked in 1998, which took lives of hundreds of Embassy staff and other innocent people. All this attacks were claimed by Al Qaeda led by the late Osama Bin Laden. Over the time and with every attack, there is a pattern in the attacks which can be exploited to forestall such attacks. Similarly, there has been noted a consistent pattern of security lapses that has allowed the attacks to be successful.

The cost of security failures usually outweighs the lessons learnt (LaPorte&Consolini ,1991). The effects of Complacency in security management are far reaching in impact and time. Great psychological devastation, loss of lives and limb, and loss of property can be debilitating in magnitude and van take years to recover from. According to Paula (2014) it seems that complacency instils a reactionary attitude. Conversely being proactive is opposed to complacency. Security practitioners should never be complacent. Binkerhoff (2001) urges homeland security practitioners responsible for emergency preparedness not to be complacent. He further urges those in charge of government institutions and corporations not to demonstrate complacency since they will be emulated by their subordinates. This underscores the overarching and critical responsibility of those in leadership and managerial positions not to allow this monster of complacency to creep in. Leading by example and enforcing rules, regulations and procedures is a critical role of those in charge of security.

II. BACKGROUND TO THE STUDY

Kenya has borne the brunt of terrorism from both Al Qaeda and its affiliate, Somali based Al Shabaab. In 2013 there was a terror attack against the Westgate Shopping Mall in Nairobi that took lives of more than 60 people from different countries across the world. The country's economy was negatively affected and citizen's trust in one another dwindled. As the Al-Qaida affiliates have continued to target the nation for its role in GWOT and the military offensive in their nations, it is now evident that the insecurity has been attributed to the increased terror and it is not limited to a particular nation. These instances of insecurity further cause instability hence impacting the world security and establish a vital need for the fruitful anti-terrorism program that enhances Global war on terror.

There have been a number of attacks against numerous critical installations in the world occasioning great losses of life and property. The 2001 attack in the United States of America is probably the most infamous attack that caught world-wide attention. Prior to 9/11, there had been attempts akin to those of 9/11 some of which were less successful and others unsuccessful. For instance, the 1995 bombing of the Murral Federal building in Oklahoma bore the hallmark of a particular tactical technique by Al Qaeda that was bound to be repeated. And in deed closer home, the 1998 Bombing of the USA embassies in Kenya and Tanzania used a similar technique to that of the Murral Federal building bombing whereby a car laden with explosives was driven into the buildings and detonated. The 1998 Kikambala Hotel bombing and the 1989 Norfolk hotel bombing are other notable examples.

Europe has also suffered from a spate of terrorist attacks. Low tech terrorism has become a preferred tactic by terrorist since it is easy to conceal from security apparatus and agencies until the fatal blow can be delivered. The use of knife attacks (London bridge stabbings), shootings at bars (niece in France), use of TATP explosives in Belgium, France and London (15 Sep 2017), running over pedestrians or crowds are examples of similar patterns of attacks that seem to catch security professionals and the public unawares. It is a fact that terrorist risks are evolving and security practitioners must always stay ahead to avoid playing catch-up. But it is also highly probable that terrorists will repeat a tactic that has proven successful. Thus, expose facto review of an incident should result in lessons learnt and more importantly development of predictive and pre-emptive capabilities to thwart future similar attempts and anticipate other modifications in attack techniques.

The Westgate Mall attack on the 23rd September 2013 brought a new tactical technique to attention of security managers. The laying siege of an installation by terrorists, who are not intent on negotiations but annihilation and martyrdom, jolted the security management psych. The Garissa University attack bore all the fingerprints of Westgate Mall style of attack. The death toll in his case went even higher than those of Westgate. Prior to Westgate and Garissa University attacks, there had been sporadic grenade and explosives attacks in Nairobi and its environs creating an atmosphere of panic and insecurity among Kenyans. On 15 January, 2019, Al Shabaab terrorists attacked Dusit2D hotel in the leafy suburb of Kileleshwa in Nairobi, Kenya. This attack bore similar tactical techniques as those of Garissa university attack, Westgate mall attack and other attacks employed by the terror group against AMISOM Targets inside Somalia. A suicide bomb attack followed by forced entry by shooting dead the guards, and finally occupying the facility and killing people inside. Though 21 lives were lost, the security agencies responded well and neutralized the 5 attackers. Through such attacks, Kenyans and other nationals lose lives and limbs and suffered great psychological trauma. Security managers are left to react rather than pre-empting the attacks. All these attacks follow a pattern that could be predictable through inference to the earlier attacks. Unfortunately, they recurred with security managers playing catch up.

Extensive research has been done in the aviation industry as pertain to complacency. Like in the aviation industry, the security industry enjoys a very little margin of error since the consequences are usually catastrophic and appalling. Investigations in the aviation industry consistently revealed that complacent human performance is responsible for human errors or a chain of events that accumulated and resulted to an accident (Paula 2014). Blue Tuna (2010) interviewed repair station managers, technicians, quality managers, and FAA inspectors, and across board, complacency ranked amongst the dirtiest dozen. Research by Grey Owl Aviation Consultants (2004) shows a 20/80 ration of accidents is attributed to human errors induced by complacency; with 20% being caused by a machine while 80 % by human error. This is quite a staggering margin and since it indicates that most accidents are attributable to human errors; and at the centre of it is complacency. Paula (2014) advices that lessons are to be learned from the extensive research in the aviation industry. The mere fact that the aviation industry has identified the problem, and over the last few decades applied efforts to understand and address it, exemplifies the credibility that complacency threat has been given in the discipline (Paula, 2014). Additionally, Paula (2014) asserts that, the fact the research has led to demonstrable improvements in organizational designs, management development and training programs directly resulting in less accidents, validates that addressing the problem can achieve positive results and may be worth the investment.

The consistent patterns of tactical techniques by risk elements that could be easily analysed and reasonably predicted, the peculiar human behaviour that smirks of complacency in relation to security matters that made the materialization of attacks by risk elements, the use of the term by security managers without proper explication either in doctrine or procedures, warrant an investigation in to the phenomenon in relation to security management. The available research done in the aviation industry can be drawn upon and related to the security management field. Finally, the only relevant research in the direction of complacency and homeland security done by Paula (2014), did not collect data from the practitioners in the field but rather did a content analysis of the secondary data. Thus, there is need to collect and analyse primary data to get a more realistic picture of the problem rather than inferential assumptions especially in Nairobi County Kenya, which has suffered numerous attacks in the past.

III. STATEMENT OF THE PROBLEM

Complacency has become the norm rather than the exception. It is a security challenge that is often recognised in rhetoric but ignored in practice. Complacency creates a security gap for exploitation by risk elements (Paula, 2014). This negatively affects security management good practices leading to massive losses in lives, property and reputations of organisation and security agencies. The psychological impact is devastating and it takes a long period of time to recover. In the bigger perspective, it creates negative security perception in a country, scares off investors, tourists etc. and leads to slump in economic growth (Blue Tuna, 2010). Unfortunately, this phenomenon has not received much scholarly attention with only a dearth of research especially in the USA.

In the recent years, attacks in Nairobi, Garissa, Mandera, Lamu etc between 2015 – 2017, bear a pattern of attack that was repeated by Al – Shabaab after initial success. Heightened security immediately after the attacks were notable but gradually slumped back to normal routine indicative of complacency. No much scholarly work has been done to explore the phenomenon of complacency in relation security management. Only a dearth of scholarly work on the concept of complacency versus security management exist. Paula L. Young (1994) took a stab at this concept as applicable to USA Homeland Security. She noted that not much had been done despite the numerous observations by high ranking government and military officials that complacency is a problem to the Homeland security. Department of Homeland security (2010) urges guarding against the dangers of complacency as the memories of 9/11 attacks and other major crises recede. The White House (2007) also makes the same cautionary remarks. The report adds that despite our best efforts, future catastrophes – natural or manmade – will occur and thus we must always remain a prepared nation (The White House, 2007). This is only a cursory glance at the phenomenon of complacency without the requisite explication on its meaning, processes, effects, and mitigation measures; without which no significant steps will be taken to deal with such a subtle but serious security challenge. There is no research on the subject in Africa and more so in Kenya yet complacency transcends every aspect of life and geolocations. Thus, the need for this study to examine complacency in the context of security management in Nairobi, Kenya.

IV. EMPIRICAL REVIEW OF LITERATURE

In a 2017 AFP article titled, “Forgetting Westgate: How Kenyans Erase Terrorism”, Tristan McConnel observes that Kenyans seem to have a propensity to amnesia about “bad things” (AFP, 2017). It has been noted that security managers and management of critical institutions such as schools, usually know about plans by nefarious individuals to cause harm but, apparently, they usually do not take necessary measures to prevent it (People Daily, 2017). This calls to question their sense of professionalism and more so the element of ‘duty of care’. Binkerhoff (2001) claims that it seems to be an American tradition to be surprised by major events such as 9/11. The same can be said of Kenyans who are mostly caught off-guard by attacks and end up engaging in blame games. It is apparent that the behaviour of Kenyans of all walks of life, including those in security management, tend to ‘sweep under the rag’ security matters once the risk has passed. This is partly due to the attempt not to revisit and relive the horrible traumatic experiences or revive debate about any tactical mistakes that could have led to the incident; both before and during such unfortunate occurrences. Furthermore, the passage of time tends to fade the memories of the event and the ensuing losses; and a sense of security creeps in, just by the mere fact that the incident has not been repeated immediately or is not likely to be repeated. However, as the White house report of 2007 rightly observes, “…despite our best efforts, future catastrophes – natural or man-made – will occur” (The White House, 2007: p.6). This is a clear declaration as well as a warning that unfortunate events will occur including risks to security and thus requiring pre-emptive steps to forestall them or mitigate them to As Low as Reasonably Practicable (ALARP). Unfortunately, we do not learn much from them and when they recur we are caught flatfooted again. Factually, the same patterns of attacks will recur albeit with small changes in the techniques since bad elements in society tend to repeat attack patterns that have been proven successful. And they exploit the gaps created by complacency on the part of the target to launch repeat attacks or attack new targets. This is despite instituting what can be called reactionary measures after attacks that serve as fist aid. It is evident from the foregoing that there is a pervasive element of what can be termed as complacency amongst the litany of security challenges.

Security Managers and professionals have constantly been warning against complacency without giving a succinct definition for its application to homeland security (Paula, 2014). Paula (2014) further surmises that complacency is a general term used by homeland security professionals to describe an attitude or human behaviour that is considered a risk to the homeland security mission. The world over, the term complacency, as related to security, has been mostly used in rhetoric without explication of the concept and its effect on security management. Use of metaphors such as “greatest risk” to security has often punctuated speeches of security managers. For it to be addressed, a contextual meaning has to be derived from analysis of security incidences that are thought to result from complacency. The security practitioners’ understanding of the concept of complacency also needs to be taken into account in deriving the contextual meaning of the term.

Complacency is not a wholly new concept to mankind. It is only that it has not been put into an organised scholarly volume that can be read, synthesised and debated by scholars and interested parties. This particularly in the security management context despite rhetorical observations by government and security professionals that it is a security challenge that has to be addressed. Other disciplines such as engineering, business management etc have made attempts to use the concept of complacency. Paula (2014) made an attempt to look into the concept as pertains to the USA Homeland Security. During development of her thesis, she encountered the challenge of scarce literature and she mostly had to rely on rhetoric; more so the homeland security doctrine, dictionaries, and even folklore, to try to explain the meaning of complacency. Indeed, up to present, there has not been much scholarly work done to explore the concept of complacency in security management context.

Of all the scholars who have attempted to define the concept of complacency, perhaps Binkerhoff (2001) gives an operationalised definition. Binkerhoff (2001) defines complacency as, "an attitude of self – satisfaction that inhibits consideration of unpleasant things and which fosters inertia of the status quo". This definition recognises that there is a psychological element that acts on the cognitive element to create an emotional state that gives preference to the status quo or a return to the status quo. The status quo in this respect is a part of the temporal aspect of complacency since the other temporal aspect is the effect of passage of time on complacency; which is not captured in the definition. However, this study will adopt this definition since it captures critical notions of self-satisfaction, attitude, psychological aspects and temporal aspects albeit in a less comprehensive manner.

According to Binkerhoff (2001) it seems to be an American tradition to be surprised by major events such as 9/11. He further indicates that Americans would not be surprised were it not for complacency and other human errors. Complacency and other human error can be considered in what scholars refer to as 'employee inappropriate behaviour'. Inappropriate employee's behaviour tends to be a common cause of organizational failure (Ericksen& Dyer, 2004). This is a recognition that despite other numerous factors, at the heart of organizational success or failure if the human element. This human element is the one that tends to suffer from the Complacency malaise. Scholars have explored the effects of complacency in various field with only a paltry of research of how the concept relates to security management. Loy (2004) alludes that a "Complacency gene" leads everyone to have a tendency to default into a careless loss of focus. This implies that complacency is inherent in the people and causes 'a careless loss of Focus'. The genetic predisposition claim needs more empirical examination, more so, how it relates to security management practices. However, experiences in the animal kingdom shows a cross cutting peculiar characteristic that exhibits some form of complacency. Take for instance an antelope that has been startled or is being chased by a predator. After running away from the risk (real or perceived), the antelope will resume grazing after a sense of safety sets in. The human animal is even quite interesting. With advanced mental capacity for decisions and rational choices, the human being will tend to forget and carry on with life as normal shortly after a risk has passed. Reactionary measures tend to be instituted shortly after an attack and the whole issues is relegated to back banners once people feel comfortably safe. Security guards will be quite vigilant and thorough in their searches during periods of risk, and shortly after, but the same diminishes after a while and casual ways of doing checks resumes.

Scholars and security managers have intimated that passage of time, an element of attitude and emotional component are responsible for development of complacency. Scholars have warned that our emotions must not be dulled by passage of time and we must maintain an unprecedented level of vigilance in everything we do (Loy, 2004). In this line of thought, it can be inferred that complacency will increase over time, is an emotion; and vigilance is antonymous to complacency (Paula, 2014). She further claims that complacency results out of habit and attitude when boredom sets in and attention shifts to other things. The passage of time creates a sense of comfort and security, group think, familiarity, boredom and eventually an attitude of mind that tends to take issues casually and carelessly. Bellavista (2005) discusses the attention cycle by describing the cyclical evolution of homeland security in public opinion and government actions regarding attacks and risks. He observes that some issues follow five predictable stages as; (1) pre-problem stage, (2) alarmed discovery stage with euphoric enthusiasm to do something, (3) awareness of the cost of making significant progress stage, (4) gradual decline of intense public interest in the problem stage that include; loss of hope due to protracted period of time taken to solve the issue, cropping up of other competing priorities and (5) post problem stage which is the return calm before the storm. Analysing stage 4, Paula (1994) implies that passage of time to creates complacency through boredom, loss of interest, loss of hope about progress or shifting attention to other more important competing issues that would require that resources are channelled to them. This supposition by Paula (2014) supports a presumption that there is a positive direct correlation between passage of time and increase in complacency. Kimery (2008) points to the same insinuation that as time moves forward, complacency increases. This should be an endeavour of statistical testing using the appropriate inferential statistical methods to ascertain such a correlation.

Closely related with the temporal aspect of complacency is the issue of competing priorities. Security plans are usually a hard sell to management since the costs of instituting security measures are mostly high. Given the fact that the amounts invested in security does not directly translate into tangible profits, management might not be inclined to pay keen attention to them. Security matters are seemingly at the bottom of the priority list and organisations tend to believe that they can be addressed when they arise and not when they are anticipated. Chertoff (2008) and Kimery (2008) are puzzled by the tendency of security professionals to recognize a potential risk and even discuss it but reserve actions until after the fact. Paula (2014) notes that over time and with fading risks, security takes a back banner and resources are re-channelled to other seemingly important areas. Lack of adequate funding eventually degrades the progress gained. This is in itself a clear manifestation of complacency since security management enterprise is an enduring and pervasive undertaking upon which other organizational activities depend. Thus, it should not be negated with the simplistic notion that it is expensive, not profitable, or the risks have receded or non-existent. The consequences of a security incident are usually far reaching and costly than the cost of investing in security preparedness. Thus, a cost- benefit analysis in this direction will highlight the need to invest in security.

Previous successes also create a sense of complacent attitude (Paula, 2014). Binkerhoff (2001) argues that self - satisfaction breeds Complacency. Successes tend to make individuals to overestimate their capabilities to influence future outcomes. This overconfidence diminishes the risk perception and in turn very minimal or no pre-emptive and preventive measures are instituted to prepare for future risks. The AMISOM experience in Somalia speaks of this predicament. The initial military actions against the enemy bore successes with the Al Shabaab losing territory and incurring heavy casualties in personnel and equipment. These initial gains against Al Shabaab created a tendency to underestimate the enemy's capabilities. This was a reinforcement of the prevalent perception that Al Shabaab is a rag tag Militia that cannot deliver a decisive blow to a professional Military. Unfortunately, the Ugandan, Burundian and Kenyan Contingents in AMISOM did eventually suffer humiliations in the hands of the hitherto ragtag Al Shabaab militia. USA experiences in Somalia Iraq and Afghanistan bear similarities to the AMISOM contingents' experiences.

Behavioural psychologists have tried to explore this phenomenon of Complacency and its development. In this respect, two concepts of self-efficacy and Optimism bias are advanced as being players in complacency. The mental element is also explored in this attempt. According to Phelps (2007) activities in two Limbic areas of the brain, the rostral anterior cingulate cortex and amygdale, reflects an optimistic attitude. This is a suggestion that psychological factors that contribute to complacency have a biological basis. Paula (2014) posits that the observation by Phelps (2007) demonstrates that people may be psychologically predisposed to complacency assuming that optimism is a psychological factor that contributes to it. According to Bandura (1994) peoples' beliefs about their capabilities to produce designated levels of performance that influences over events that determines how people feel think, motivate themselves and believes creates a sense of self – efficacy and thus creates overconfidence. Scholarly literature concludes that people believes have the ability to affect the outcome of a situation and believe that they can make the result one in which they desire it to be (Paula, 2014). This is a concept of optimism that reflects personal or group desires about the outcome of an event or situation. Literature broadly accepted by psychologists indicate that people are naturally prone to be optimistic even with the knowledge of prevailing risks (Paula, 2014). Personal or group desire in some way guides the optimistic tendencies of individuals leading to complacency. A 2009 study in the University of Kansas finds that despite calamities from economic recession, wars and famine to a flu epidemic afflicting the earth... humans are by nature optimistic. Security practitioners may be naturally prone towards optimism bias despite the awareness of dangers.

A combination of optimism and self-efficacy can contribute to an attitude of complacency. As Paula (2014) argues, individuals' high optimism (Optimism bias) about outcomes and the ability they have to affect the outcomes (Self-efficacy) can lead to a feeling of confidence or self-satisfaction. This argument presumes the possibility of optimism bias overshadowing self-efficacy that leading to false sense of self satisfaction or confidence in individual or group capabilities. This in essence is part of the core components of the definition of complacency as provided by Binkerhoff (2001).

The weight of an individual's responsibility also plays a part in the degree of complacency in an individual or organization. The greater the individual's security responsibility, the less complacent they are and vice versa. Paula (2014) notes where an individual falls within the homeland security enterprise and differs based on their individual responsibilities. It evident in every day undertakings that security professionals exhibit varying degrees of complacency depending upon what their responsibilities are in where they fit in the enterprise. Senior leadership usually carry the biggest burden of responsibility which tends to lessen down the hierarchy. The management is expected to own up to security mishaps and even resign or be prosecuted. Such negative motivators of an unpleasant consequences keep them on toes in ensuring that security lapses are kept as low as reasonably possible (ALARP).

On the other hand, with knowledge of the amount of accountability, junior security professionals tend to be more complacent since they know the bosses will have to carry the cross. They gloss over security procedures and protocols and overlook what is acceptable as good security practices. On the flip side, this hypothesis would not hold in the case where the casualty counts and likelihood is considered. In the even that as security incident occurs, it is the junior security person at the immediate scene that will suffer either death or injury while the senior management will have to suffer psychological duress due to being held to account. Thus, with this realisation, it is expected that all levels of the security hierarchy must not be complacent since the effects are equally undesirable at all levels. More so the hands-on security guard or low-ranking security manager, whose life and limb are at stake, should be the most vigilant.

Geographical proximity to danger has been observed to account for instances of complacency in security management. The variation in the risk levels from place to place makes people in less risked areas to be less vigilant as compared to those in more risked areas. Citing a speech by the former USA counterterrorism Tsar, Richard Clarke, Kimery (2008) points out that since 9/11 there has been, in some parts of the country and in popular opinion, a growing sense of complacency. Paula (2014) analysed this assertion to mean that "…in some places…" implied a geographical location; that in some areas people tended to be more complacent than in other areas. This has been evident in Kenya with citizens and security professionals being more vigilant and cautious in risk prone areas such as the North-Eastern Kenya and Coastal areas risked by Al Shabaab or North-western risked by cattle rustling and highway robberies. In Nairobi city, certain alleys will attract caution and vigilance since the likelihood of being robbed as opposed to certain areas of the city. Thus, there is an element of complacency in areas of less risks whereas areas of high risks people are likely to be less complacent.

Demotivated employees are likely to be complacent. Some of the critical motivational aspects in the security management enterprise are remuneration and promotions. Remuneration has long been touted to be factor in employee motivation. Henri Fayol (1949) points out that among others, remuneration is a principle of management. Well remunerated security practitioners are bound to apply themselves to their duties with minimal complacency. Career progression is also critical since employees who are not promoted when due will be disillusioned about their future in the organization and tend to do things with don't - care attitude. Promotions also comes with higher responsibilities and thus the employee will tend to get less complacent as he/she becomes more accountable as they move up the hierarchical ladder.

Overconfidence in one's training, skills and experience contributes to instances of complacency. This is what Denning (2006) refers to as "expert arrogance". According to Denning (2006), expert arrogance s listed as one of the causes of complacency in the aviation industry. Jensen explains that experts tend to disdain laymen or experts in other fields. This is a perennial tendency of experts. The fact that the expert is right more often than the laymen can lead to the illusion of always being right (Denning, 2006). Such an attitude will discourage diverse inputs that can enable spotting of a security problem. Weiner (1981) offers a startling observation that things that things that should prevent accidents, such as experience, training and knowledge, contributes to complacency. This can evident in instances in which security professionals ignore security procedures and protocols, rush through security checklists, use shortcuts, employ poor judgement. Such behaviours spell the difference between hazardous performance and professional performance (Weiner, 1981). This is disconcerting but an evident phenomenon that is present in individuals in an organization. In another angle, overconfidence in a worker's expertise will lead to what Jensen (1995) terms as dependency complacency. this is a situation where some employees tend to rely on others to perform certain tasks because they are perceived to be knowledgeable in them and cam do the job well. This leads to misplaced confidence in the "expert co-worker" to catch all the mistakes and thus workers tend not to do their work properly and conscientiously.

According to Jensen (1995) and Denning (2006) technology can lead to complacency. Technology leads to changes in roles of employees from main operators to mere supervisors (Jensen, 1995). Both Jensen (1995) and Denning (2006) recognise the tendency of employees to in the infallibility of the automated machines. Employees are lulled to think that computers will not make mistakes and will perform everything well. Computerized safety systems require constant monitoring. Closed Circuit Television (CCTV) will require manning so as to detect intrusion or other forms of security breaches and possibly instituted remedial measures. The machines in themselves can only detect or record but might not be able to take remedial steps. Therefore, a CCTV operator who thinks the cameras will record everything will be tempted to take a nap or even leave the machine unattended. Other security technologies, just like the CCTV example, will require the constant monitoring.

According to Denning (2006), over-accentuating of the positive leads to complacency. this attitude leads security managers and organization to ignore sceptics and naysayers and exclusively focus on the positive. This is what I call “inspirational speaker syndrome”. This creates what Denning (2006) also refers as a “Black - Swan bias”; which is a focus on what is expected and negating other possibilities. The mind-set is of the “can – do” perspective and anything to the contrary is dismissed and thus the possibility of ignoring merit in a varying viewpoint. Most high value knowledge lies in the negatives that reveals the pitfalls, difficulties and obstacles that lies in the way of success (Denning, 2006). However, security and organizational managers can see such narrative as a risk to the management plans and objectives, thus Denning (2006) indicate that fear of negative career consequences can hamper their dissemination. Unfortunately, when disaster strikes as a results of ignoring indicators and warnings, it becomes a blame game situation. The Westgate attack of September 2013 in Kenya is an example. After the attack, the public was treated to an unfortunate soap opera of finger pointing amongst the security services. Intelligence agencies were accused of not sharing information with the relevant executory security agencies in time while the intelligence agencies vehemently defended themselves against such disparaging allegations. But in sum, that could not reverse the fact that life, limb and property were loss and that such consequences were irreversible.

According to Jensen (1995) and Denning (2006) organizational setup creates complacency through the creeping in of a group think mentality. Denning (2006) notes that group think occurs when people are deeply involved in a cohesive group whose striving for unanimity overrides a realistic appraisal of alternative courses of action. Large organizations often exhibit symptoms of group think, including illusions of invulnerability and a sense of superiority, collective rationalization and stereotyping of outsiders as uninformed, ignoring contrary data, suppressing alternative viewpoints and shielding leadership from dissent (Denning, 2006).

Jennings (1995) indicts large organizations for precipitation organization induced complacency. According to Jensen (1995) this form of organizational group think occurs when; poor management sets in and it fails to hold people accountable for their wrong actions at work, management becomes satisfied with mediocre performance, workers have the propensity to break rules and take shortcuts in performing their tasks assuming that the will not be punished,, subpar working style becomes the norm, non-productive workers are permitted to continue working and keep making errors, personnel stop reporting errors at work, and eventually productive workers who are creative and care for the company become complacent at their tasks. These observations seem to support the notion of employees feeling comfortable with the environment and start conducting business casually or due to over familiarization with management who become less and less strict on their “pals”. Monotony of the work and work environment also accounts in part to this organizational induced groupthink and complacency. This is especially after a period of intense and mentally stimulating work period or during the occurrence of a risk situation. Thereafter, the workers will take a low-key attitude with the thought that the worst is over (Jensen, 1995). At these instances, the vigilance of security personnel is significantly reduced and guard is let down. This will cause the security practitioners not to be able to react appropriately to a new and sudden inject of action or security risk.

Mental stress and fatigue also account for increased instances of complacency. Mental stress does affect the psychological aspects of the individual and creates distractions. Similarly, fatigue impacts on the mental and physical aspects of the individual and thus rendering them inattentive and ineffective in performing, for instance, security duties. Jensen (1995) notes that employees faced with fatigue or stress due to external factors such as insufficient sleep and marital problems will not be in the right frame of mind or physical disposition to perform their tasks. Hallucination is also likely to set in in such conditions of mental stress and fatigue. They will, for instance, not be as meticulous and pay attention less attention to certain seemingly mundane tasks. They can also become complacent and begin to see and hear what they expect to see and hear in a given scenario, instead of what is actually transpiring in the real scenario (Jensen, 1995).

Complacency can be good or bad depending on who is being complacent (Binkerhoff, 2001). If it is the Citizenry, then it is an indicator of success on the part of those responsible for security. In any case it is the duty of a government to assure security of its people and reduce their security worries. If it is the prevalent attitude of people require to pay attention to unpleasant things, then it becomes a problem. Public administration practitioners do not expect bureaucracies to be error free and acknowledge that people make mistakes and machines break (Paula, 2014). The world of security management also does not expect an error free scenario but a reasonable anticipation of risks and development of countermeasures. As LaPorte&Consolini (1991) observe, no one is perfect and no organisation is able to achieve its ideals. Bureaucratic Folklore teaches us that error making is normal in a bureaucratic condition yet some organizations must not make serious mistakes because their work is too important and the effects of their failure is too disastrous (Paula, 2014). These organizations are, but not limited to, Military, Police, Intelligence agencies, Security firms, Aviation industry, National

Disaster Management bodies etc. Security in a country is paramount in creating the safe conditions in which the political, social and economic aspects can thrive. Therefore, security lapses of all manner including complacency should be vehemently resisted.

The cost of security failures usually outweighs the lessons learnt (LaPorte&Consolini ,1991). The effects of Complacency in security management are far reaching in impact and time. Great psychological devastation, loss of lives and limb, and loss of property can be debilitating in magnitude and van take years to recover from. According to Paula (2014) it seems that complacency instils a reactionary attitude. Conversely being proactive is opposed to complacency. Security practitioners should never be complacent. Binkerhoff (2001) urges homeland security practitioners responsible for emergency preparedness not to be complacent. He further urges those in charge of government institutions and corporations not to demonstrate complacency since they will be emulated by their subordinates. This underscores the overarching and critical responsibility of those in leadership and managerial positions not to allow this monster of complacency to creep in. Leading by example and enforcing rules, regulations and procedures is a critical role of those in charge of security.

V. THEORETICAL FRAMEWORK

Routine activity theory was used to explain how complacency weaves into the daily routine behaviour of security managers and practitioners and thus nefarious elements can exploit such situations. Postulated by Felson and Cohen (1967) Routine activity theories contends that there are three conditions which should be present for a crime or attack to occur. The these are the target, opportunity and lack of an able guardian. While the target is usually present, effective security managers in their undertakings must reduce the latter two to As Low as Reasonably Practicable (ALARP). Complacency tends to increase the opportunity for attack by presenting a situation and notion of absence of a capable guardian. And where the guardian is present, then he/she is seen to take for granted security of the asset/target and thus still present an opportunity for attack. This theory entails in it some elements of the Rational Choice theory in that through careful surveillance and analysis, the attacker is able to pick the elements of complacency that create an opportunity for a successful attack; inflicting maximum damage on the target at minimal cost to the attacker.

VI. METHODOLOGY

The primary method in this study was quantitative survey. Questions were delivered verbally due to the widespread prevalence sensitivity of the topic under study. Besides, numerous individuals in Kenya, both government officials and citizens, still do not have an in-depth comprehension of insecurity. Without a doubt, terrorism is relatively new in Kenya, and numerous individuals are still coming to terms with the fact that it exists. Therefore, giving the questions verbally will give the researcher a good opportunity to explain each concept regarding terrorism. A random stratified sampling method was utilized to draw a representative sample from each supposed by the researcher to be representative of the diversity needed in the study. The researcher adopted verbal interviews and questionnaires as the main tools for data collection. The researcher used descriptive research design.

Research design is the blueprint used to guide a research study to ensure that it addresses the research problem. It provides a framework that guides the determination of the data to be collected, how it is collected and analyzed. The study therefore employed a descriptive research design. A descriptive, research design involves collecting and analyzing study unit data at a point in time or over short to medium-term time horizon in order to assess strength of relationships among variables. The target population of this study was the personnel at ministries of foreign affairs, trade, immigration and planning. The study targeted 500 respondents

Table 1. ***Target Population***

Population Category	Population frequency	Percent
National Police service	100	20
Kenya Wildlife Services	200	40
Kenya Forest Service	100	20
Private security services	100	20
Total	500	100

VII. STUDY FINDINGS

Complacency of Security Managers

The study participants were asked if the institution managers understand the meaning of Complacency in the context of managing security. Majority of respondents (65%) revealed that the management have comprehensive information about complacency. This has played an essential role in curbing insecurity in the city. They also indicated that the managers always use the term complacency in their security briefing without necessarily explicating as to what it means or entails. The management has also helped in educating employees about the importance of security competence, this might be one of the reasons as why the number of insecurities has decreased significantly in the past few months.

Factors Affect Complacency in the Context of Security Management

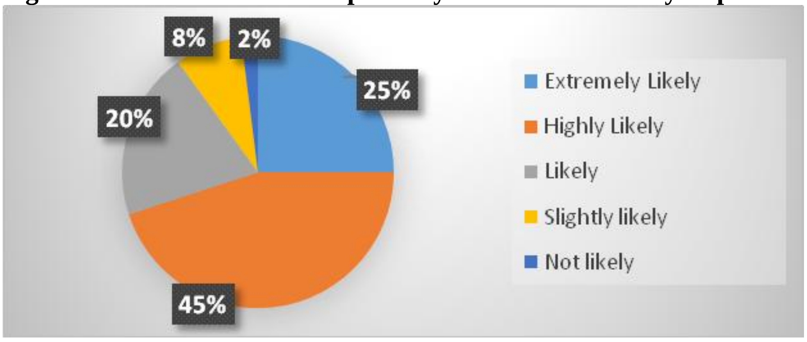
Table 2 below depicts the respondents' views on the effects of selected factors on complacency of security managers in security management practices:

Table 2.*Factors Affect Complacency in the Context of Security Management*

Factor	Complacency increased	Complacency decreased	Don't know	Any other (Indicate)
Passage of time	49.3%	37.0%	0.7%	13.0%
Individual's genetic make-up	52.2%	41.3%	0.7%	5.8%
Human attention span	55.8%	37.7%	0.0%	6.5%
Effects of Competing security priorities on security budget	1.7%	44.2%	42.0%	11.6%
Success in preventing previous attacks	43.5%	44.9%	2.2%	9.4%
Increased security officer's workload	47.8%	44.9%	5.1%	2.2%
Proximity to risky areas	44.9%	47.1%	8.0%	0.0%
Demotivated security officers	53.3%	38.7 %	6.6%	1.5%
Over-confidence in one's security training	33.3%	56.5%	13.0%	2.9%
Change of role from security operator to security supervisor	42.0%	47.1%	8.0%	2.9%
Overemphasis/accentuation of previous success in security management	55.8%	40.6%	2.2%	1.4%
Mental and physical fatigue/ tiredness	47.1%	44.2%	8.7%	0.0%
Organizational set-up that encourage group think and social loafing	57.2%	39.1%	3.6%	0.0%

The Table above present factors affect complacency in the context of security management. Majority (49.3%, 52.2% and 55.8%) of respondent's reveled passage of time, Individual's genetic make-up and Human attention span affects the complacency in the context of security management respectively. The findings also show that 44.9%, 47.1%, 53.3%, 56.5% and 47.1% of study participants that success in preventing previous attacks, increased security officer's workload, proximity to risky areas, demotivated security officers, over-confidence in one's security training and change of role from security operator to security supervisor negatively affects complacency respectively. The table also indicated that 55.8%, 47.1% and 57.2% of participants reported that overemphasis/accentuation of previous success in security management, mental and physical fatigue/ tiredness and organizational set-up that encourage group think and social loafing increases complacency.

Figure 1. Likelihood that Complacency can lead to Security Lapses



The Figure above shows the likelihood of complacency leading to collapse of security. The findings show that majority (45%) of respondents indicated that complacency has a high likelihood of leading to security lapses while 25% indicated that complacency has an extreme likelihood of leading to security lapses. 20% of the respondents indicated that complacency leads to a likelihood of security lapses, 8 % indicated that it can lead to a slight likelihood of security lapses while 2% said complacency will not likely lead to security Lapses. The findings indicate that complacency can indeed lead to instances of security breaches.

Measures to Reduce Complacency in security management

The respondents were provided with a list of possible measures to reduce complacency in security management and they were asked to indicate if they could be effective. The findings are presented below:

Table 3: Measures to Reduce Complacency in security management

	Yes	No
Training	54%	46%
Prosecution for negligence	64%	36%
Summary/ Administrative discipline	78%	22.0%
Transfers/Postings	68%	32%
Pay Increase	41%	59%
Reduced working hours (Work load)	72%	28%

From the Table above majority (54%, 64% and 78%) of respondents revealed that training, prosecution for negligence and summary/ administrative discipline can be effective in reducing complacency in security management. From the table 68% and 72% stated that transfers/postings and reduced working hours (Work load) reduces complacency while 59%

VIII. Discussion

The study found out that majority if security managers in Kenya (65%) have been using the term ‘Complacency’ or its synonyms in their security briefings without necessarily making it clear as to what it meant or entailed. It is worth noting that if the recipient in the communication chain does not understand the language in use then communication is not taking place and thus it will be difficult to respond of act. Thus, in this case, it will be futile to expect the security officers to change their mind-set on the issue of complacency when they do not know it meaning and effect on security management practices. Repeating it and making it a buzzword does substitute and instructive explanation.

It was also found out that certain factors encourage complacency more than others with organisational setting that promote group think, over accentuating past successes, reduced attention span over time, human genetic makeup and demotivated security officers being at the top of the list at 57.2%,55.8%, 55.8%, 52.2% and 53.3% respectively. However, more studies using experimental research design will be essential in confirm such findings.

The study further found that complacency will highly likely lead to security lapses/ breaches with 45% of the respondents affirming the same. This has been witnessed in many countries. Using Kenya as an example, the country has suffered many attacks in the past and it is observable that despite such attacks, the security agencies tend to relax their guard a while after the attack. This has allowed attacks bearing the same tactical techniques to be used again against other targets. For instance, the resemblance in the modus operandi used to attack Westgate mall in 2013, was repeated in the Moi University, Garissa Campus attack in 2015 and recently the Dusit2D Hotel attack in January 2019.

Finally, the study established that among possible measures to reduce instances of complacency in security management, summary/administrative discipline, reduced working hours in a shift, transfers, prosecution of security managers for negligence and training ranked higher with 78%, 72%, 68%, 64% and 54% respectively. The preference in complacency reducing measures indicates a high importance being placed on the internal administrative disciplinary action. This could be due to the need to safe face of the culprit security professional. However, training is being given a lower rating whereas is it a crucial facet of security management that serves to keep the security operatives' skills current and in tandem with the emergent and dynamic security threats.

IX. CONCLUSION

The study concludes that whereas complacency has been identified as security threat due to the effects it has on security management practices, the phenomenon has not been addressed with the seriousness it deserves. Whereas technological improvements have been made on areas such as CCTV, metal and explosives detectors, intrusion detection systems and alarms, information security measures, etc., it should not be lost to security managers that the human element is still critical and is the one that monitors and ensures that the advanced technologies are working. It is this very element that is affected by complacent behaviour and thus rendering the technology ineffective. Therefore, the issue of complacency has to be addressed in a serious manner through training and research so as to ensure that the most critical component of the security equation delivers at optimum capacity at all time. The beginning is the understanding of the phenomenon as it relates to security management. Knowledge and expertise can be drawn from various fields such as psychology, aviation, etc. The effects of complacency in security management need to be established so as to form a basis of formulation of remedial measures and training is security operatives.

X. RECOMMENDATIONS

From the findings of the study, it is recommended that the following be instituted to address complacency it the security management filed:

a. In-depth research using experimental design be conducted to understand complacency in security management as it affects individuals and security management practices.
b. Following from the research, appropriate countermeasures, that are not limited to those in the findings of this study, be formulated and form a basis for review of security policies and procedures. The burden of 'duty of care' should weigh heavily on the individual security person where negligence is proven.
c. Training and refresher of security operatives on security scenarios will serve not only to update their skills but also to minimize complacency.

XI. ACKNOWLEDGEMENTS

I acknowledge the invaluable insights and Guidance accorded to me by my supervisors, Professor Simon MwangiWokabi and Doctor Eric Kiprono Bor.

REFERENCES

[1] AFP (2017). *Forgetting Westgate: How Kenyans Erase Terrorism*. An article by Tristan McConnel; available at https://www.yahoo.com/news/foorgetting-westagate-kenya-erases-terrorism-015749536.html accessed om 10 September 2017.
[2] Akers Jr, F. H., & Singleton, G. B. (2000). Task Force Ranger: A Case Study Examining the Application of Advanced Technologies in Modern Urban Warfare. *National Security Program Office, USDOE, Oakridge, TN November*.
[3] Anderson, P. (1999). Complexity theory and organization science. Special Issue: Application of Complexity Theory to Organization Science. *Organization Science, 10*(3), 216–232.
[4] Anderson, P., Meyer, A., Eisenhardt, K., Carley, K. &Pettigrew, A. (1999). Introduction to the special issue: Applications of complexity theory to organization

science. Special Issue: Application of Complexity Theory to Organization Science. *Organization Science*, *10*(3), 233–236.

[5] Bandura, A. (1994). Self-efficacy. *The encyclopedia of human behavior*, *4*, 71– 81.

[6] Bellavita, C. (2005). Changing homeland security: The issue-attention cycle. *Homeland Security Affairs*, *1*(1).

[7] Blue Tuna. (2010). *The curse of complacency*. Retrieved from http://www.bluetunadocs.com/CurseofComplacency.html

[8] Brinkerhoff, J. (2001, December). The relationship of warning and response in homeland security. *Journal of Homeland Security*, 1–8.

[9] Chibuike, U. C., &Eme, O. I. (2019). Terrorism & its Socio-Economic Effects in Nigeria. *Journal of Contemporary Research in Social Sciences*, *1*(1), 97-113.

[10] Department of Homeland Security. (2009, May 6). *Remarks by secretaryNapolitano by today's media briefing on the H1N1 flu outbreak.* Retrieved from https://www.dhs.gov/news/2009/05/06/secretary-napolitanosremarks-h1n1-flu-outbreak-media-briefing.

[11] Department of Homeland Security. (2010). *Quadrennial homeland security review.* Washington, DC: Government Printing Office. *Educational resources, definitions of human factors and ergonomics*. (n.d.).Retrieved from Human Factors and Ergonomics Society website:http://www.hfes.org/web/educationalresources/hfedefinitionsmain.html

[12] Dekker, S., &Hollnagel, E. (2004). Human factors and folk models. *Cognition, Technology & Work*, *6*(2), 79–86.

[13] Denning, S. (2006). Challenging complacency. *Ask Magazine*, 46–51.

[14] Fayol, H. (1949). *General and Industrial Management*. Pitman Publishing Limited, London, England.

[15] Freilich, J. D., &LaFree, G. (2015). Criminology theory and terrorism: Introduction to the special issue.

[16] Grey Owl Aviation Consultants. (2004). *Complacency*. Retrieved from http://www.greyowl.com/articles/complac_article.pdf.

[17] Greenberg, J., Solomon, S., &Pyszczynski, T. (1997). Terror management theory of self-esteem and cultural worldviews: Empirical assessments and conceptual refinements. *Advances in experimental social psychology*, *29*, 61-139.

[18] Jensen, R. S. (1995). *Pilot judgment and crew resource management.* Aldershot, UK: Avebury Aviation.

[19] Kimery, A. (2008). *Chertoff warns of complacency over home front preparedness*. Retrieved from:http://www.hstoday.us/briefings/industrynews/singlearticle/Chertoff-warns-of-complacency-overhomefront-preparedness/97b734fe06e7c0946827885d89851595.html

[20] LaPorte, T. R., &Consolini, P. M. (1991, January). Working in practice but not in theory: Theoretical challenges of "high reliability organizations." *Journal ofPublic Administration Research and Theory: J-PART, (1)*1, 19–48.

[21] Loy, J. (2004). *Remarks by deputy secretary of homeland security James Loy at the national cargo Security Council annual convention*. LasVegas, NV.

[22] Macready, J. D. (2016). Hannah Arendt and the political meaning of human dignity. *Journal of Social Philosophy*, *47*(4), 399-419.

[23] Omale, J. O. (2016). Terrorism in Nigeria: Theories and Practice.

[24] Onuoha, F. C. (2012). The audacity of the Boko Haram: Background, analysis and emerging trend. *Security Journal*, *25*(2), 134-151.

[25] Osborne, M. (2014). *Ethnicity and Empire in Kenya: Loyalty and Martial Race among the Akamba, c. 1800 to the Present*. Cambridge University Press.

[26] Oxford English Dictionary. (2010). Complacency. Second edition, 1989. Online version November 2010. Earlier version first published in New English Dictionary, 1891. Retrieved from http://www.oed.com:80/Entry/37605.

[27] Paula L. Y. P. (2014). Complacency: *Risk to Homeland Security*. A Published Master's Thesis presented to the Naval Postgraduate School; Cleveland state University, USA.

[28] People Daily (2017). *School Knew of Girls Arson Plot, Say Sleuths*. An article by Sandra Wekesa in the people Daily Newspaper of 11 September 2017. Issue No 06392. Nairobi, Kenya.

[29] Rudolph Jr, J. R. (Ed.). (2015). *Encyclopedia of Modern Ethnic Conflicts, [2 volumes]*. ABC-CLIO.

[30] Teddlie, C., &Tashakkori, A. (2010). Overview of contemporary issues in mixed methods research. *Handbook of mixed methods in social and behavioral research*, 1-41.

[31] Webster Online Dictionary. (2011). *Complacency*. Retrieved from http://www. merriam-webster.com/dictionary/complacency.

[32] White House, The. Homeland Security Council. (2007). National *strategy for homeland security*. Washington, DC: Government Printing Office.

[33] Ziemelis, K. (2001). Complex systems-nature insight review. *Nature 410*, 242– 258.