Journal of Information and Technology

Information System Security Mechanisms in Finacial Management

Wilfred Kakucha & Ishaq Buya

Stratford Peer Reviewed Journals and Book Publishing
Journal of Information & Technology
Volume 2||Issue 1||Page 1- 16|March||2018|
Email: stratfordjournals.org

Information System Security Mechanisms in Financial Management

[*] [1]Wilfred Kakucha & [2] Ishaq Buya

[1*]PhD Candidate, Jomo Kenyatta University of Agriculture and Technology

[2]PhD Candidate, Jomo Kenyatta University of Agriculture and Technology

***E-mail of corresponding author:** wilfredkakucha@yahoo.com

***How to cite this article*: Kakucha, W., & Buya, I., (2018), *Information System Security Mechanisms in Financial Management, Journal of Information and Technology* Vol 2(1) pp. 1-16.**

Abstract

Organizations and people that use computers can describe their needs for information security and trust in systems in terms of three major requirements which are confidentiality, integrity and availability. Payroll and general ledger were among the first processes to become automated. However, organizations have continuously experienced targeted attacks and on an increasingly frequent basis. Security risk is increasing due to increased internal and external threats. Subsequently, security is getting harder to manage. In this climate, organizations must employ strategies to direct their security efforts and should optimize their limited resources. The study endeared to analyze and evaluate security strategies utilized in the financial management systems with the sole aim of driving innovation and generating competitive advantage. The researcher utilized desktop literature review, this type of review critiques and summarizes a body of literature and draws conclusions about the topic in question. The study found that many organizations operate in large-scale network environments with numerous servers, fixed terminals and portable wireless devices including laptops and smart phones. In addition, there are employees with complex access profiles to masses of information at varying levels of sensitivity. The strategies focused on security risk management include prevention, deterrence, surveillance, detection, response, deception, perimeter defense and layering. Of importance is the loss prevention which focuses on what critical assets are and how they can be protected. Attacks can be prevented by employing these strategies and the improvement of system efficiency. The study recommended that strategies should be devised to contend with risk exposure in financial security environments which requires a systematic and comprehensive approach with a view to learning and developing situational awareness especially from security incidents.

Keywords*: Security, Strategy, Information system, Financial Management and Organization*

1.0 Introduction

1.1 Background of the Study

The need for information security has become necessary over the years, with the automation of routine clerical functions, specifically accounting functions. Organizations and people that use computers can describe their needs for information security and trust in systems in terms of three major requirements which are confidentiality, integrity and availability. Payroll and general ledger were among the first processes to become automated. As computers became more powerful and more widespread, information systems grew to support almost every business process. Data networks also grew in this period, and have been increasingly used to support business communications (Von Solms, 2010). Data communications allowed an increasing internal integration of far-flung business processes hence exposing systems to security threats. Data communications have tied businesses more closely to their suppliers and customers (Kim, 2014). Starting with the first Electronic Data Interchange (EDI) systems of the 1970s, commerce became synonymous with data networks. The speed and volume of data has increased dramatically, as has the scope of the partners with which data is exchanged and the depth to which internal systems are exposed to trading partners (Bowen *et.al* 2003).

According to Mattord (2011) the security concerns of an organization might include the following: Financial practices not only include fraud or theft, but also good governance, compliance, accountability and audit Industrial which involves protection of assets from espionage, theft, sabotage; security of supply (materials, energy), second sourcing and secure transport of assets. Staff or customers premises such as access controls, secure stores, surveillance, intruder detection and outsourced facilities management, is also a security concern to an organization (Hendriks, 2013). Individual protection of customers, staff, partners and suppliers from hazardous substances or environments; safety and welfare in the workplace freedom from discrimination, intimidation and bullying; immunity from legal action when acting on behalf of the company and educational (awareness programs, regular communications, training and drills) are some of the security concerns an organization should deal with (Rodin-Brown, 2008).

Information Security therefore is the active protection of information, however stored or conveyed, to ensure it is available only to authorized users at the time they require it, with appropriate levels of integrity. This is normally achieved through an Information Security Management system (ISMS) (Sabahi, 2011). To address these security risks, an organization must implement an information security strategy through the establishment of a comprehensive framework to enable the development, institutionalization, assessment, and improvement of an information security program. In particular, the information security strategy must support the overall organization’s strategic plans with its content clearly traceable to these higher-level sources (Bowen *et al.* 2006).

While organizations typically deploy ‘baseline’ security measures, the number of security incidents continues to increase (Rebollo, 2015). Over 60% of organizations are employing technical information security counter measures, including anti-virus software, firewalls, anti-spyware software, virtual private networks (VPN’s), vulnerability/patch management, encryption of data in transit, and intrusion detection systems (Richardson 2011; Kessel 2011). However these reports also point out that organizations have experienced targeted attacks continuously and on an increasingly frequent basis. Further, these same studies show that security risk is increasing due to increased internal and external threats. Subsequently, security is getting harder to manage.

However, besides prevention, there are a number of security strategies conceptually identified in literature, such as: detection, deterrence, and deception (Tirenin and Faatz 1999). There has been little field-work conducted to determine which security strategies are employed by organizations to address the range of security risks, and how these strategies are deployed. Therefore, this paper poses the following exploratory research question ‘How can organizations use security strategies to protect information systems?

1.2 Statement of the Problem

Organizations have continuously experienced targeted attacks and on an increasingly frequent basis. Security risk is increasing due to increased internal and external threats. Subsequently, security is getting harder to manage. In this climate, organizations must employ strategies to direct their security efforts and should optimize their limited resources (Edwards & Willimas 2001; Saydjari 2004; Anderson & Choobineha 2008). However a single strategy may not be enough. Richards and Davis (2010) argue, that organizations should utilize multiple information security strategies in order to ensure effectiveness of security measures and to maintain security policies.

Besides prevention, there are a number of security strategies conceptually identified in literature, such as: detection, deterrence, and deception. There has been little field-work conducted to determine which security strategies are employed by organizations to address the range of security risks, and how these strategies are deployed. Premised on this fact, the current study focused analyzing and evaluating security strategies that are effective in financial management systems.

1.3 Purpose of the Study

To analyze and evaluate security strategies utilized in the financial management systems with the sole aim of driving innovation and generating competitive advantage.

2.0 Methodology

The researcher utilized desktop literature review, this type of review critiques and summarizes a body of literature and draws conclusions about the topic in question. The body of literature is made up of the relevant studies and knowledge that address the subject area. It is typically selective in the material it uses, although the criteria for selecting specific sources for review are not always apparent to the reader. This type of review is useful in gathering together a volume of literature in a specific subject area and summarizing and synthesizing it.

3.0 Findings and Discussion on Information Security Mechanisms

3.1 The Security Management Process

The security management process consists of activities that are carried out by the security management itself or activities that are controlled by the security management. Because organizations and their information systems constantly change, the activities within the security management process must be revised continuously, in order to stay up-to-date and effective. Security management is a continuous process and it can be compared to W. Edwards Deming's Quality Circle (Plan, Do, Check, Act) (Ohno *et al*. 2005).

The inputs are the requirements which are formed by the clients. The requirements are translated into security services, security quality that needs to be provided in the security section of the service level agreements. This means that both the client and the plan sub-process have inputs in the Service Level Agreement (SLA) and the SLA is an input for both the client and the process. The provider then develops the security plans for his/her organization. These security plans contain the security policies and the operational level agreements (Schwalbe, 2015).

According to Liu (2005); Artail (2006) and Ruiu (2006) the security plans (Plan) are then implemented and the implementation is then evaluated. After the evaluation then both the plans and the implementation of the plan are maintained. The activities, results/products and the process are documented. External reports are written and sent to the clients. The clients are then able to adapt their requirements based on the information received through the reports. Furthermore, the service provider can adjust their plan or the implementation based on their findings in order to satisfy all the requirements stated in the SLA (including new requirements).

3.1.1. Control

The first activity in the security management process is the “Control” sub-process. The Control sub-process organizes and manages the security management process itself. The Control sub-process defines the processes, the allocation of responsibility for the policy statements and the management framework (Henauer 2003; Rytz *et al*. 2003).

The security management framework defines the sub-processes for the development of security plans, the implementation of the security plans, the evaluation and how the results of the evaluations are translated into action plans. Furthermore, the management framework defines how should be reported to clients (Stolfo, 2004). An effective program of management controls is needed to cover all aspects of information security, including physical security, classification of information, the means of recovering from breaches of security, and above all training to instill awareness and acceptance by people. The activities that take place in the Control process are summed up in the following table, which contains the name of the (sub) activity and a short definition of the activity.

Table 1: Activities in the Control Process of Security Management

Activities	Sub-Activities	Descriptions
	Implement Control policies	This process outlines the specific requirements and rules that have to be met in order to implement security management. The process ends with *policy statement*.
	Set up the security organization	This process sets up the organizations for information security. For example in this process the structure the responsibilities are set up. This process ends with *security management framework*.
	Reporting	In this process the whole targeting process is documented in a specific way. This process ends with *reports*.

3.1.2. Security Risk Management

Management of security risks applies the principles of risk management to the management of security threats. It consists of identifying threats (or risk causes), assessing the effectiveness of existing controls to face those threats, determining the risks' consequence(s), prioritizing the risks by rating the likelihood and impact, classifying the type of risk and selecting and appropriate risk option or risk response.

3.1.3 Loss Prevention

Loss prevention focuses on what your critical assets are and how you are going to protect them. A key component to loss prevention is assessing the potential threats to the successful achievement of the goal. This must include the potential opportunities that further the object (why take the risk unless there's an upside?) Balance probability and impact determine and implement measures to minimize or eliminate those threats (Richardson, 2008).

3.2 Security Risk Management Strategies

Information security is one such strategic component. An increase in the breadth, scope, and depth of information sharing across organizations elevates the importance of protecting this information. Protecting shared electronic commerce information is more than simply restricting access to only authorized parties. Dourish and Redmiles (2002) states that trustworthiness of the information as bound into a business transaction must be established and maintained. Similar issues have always existed with highly integrated systems used solely for internal support (Snyder, 2006). Management often evades these issues, assuming that physical and administrative controls can compensate for inadequate technical security. Internal information systems may lack sophisticated technical security controls but still perform adequately as long as equipment and communications are physically secured, and as long as only properly managed internal staff may access the system. Opening systems to external parties to vendors, customers, and even potential customers among the public at large negates the physical and administrative controls. Technical security controls are explicitly required to maintain the trust relationships that organizations rely upon.

Security strategy in the age of electronic commerce focuses on building business trust relationships in which the relationship itself is based on no more than electronic signals. The traditional information security values of confidentiality, integrity, and availability are incorporated into complex trust relationships based on data communication protocols (Zhang, 2015).

Information security's role in strategy has evolved from the keeper of secrets to the builder of electronic trust networks. Ensuring that information security provides the maximum strategic benefit to the organization requires a further evolution, from trust architect to information steward. Where information can be assigned value in supporting organizational goals, the efficient management of this value can provide greater benefit to the organization. Just as with any other productive asset, information should be identified, measured, and properly channeled to its most valued use (Andres, 2012). This view of information is a break with most organization's current practice, and requires that an economic and business process model be applied to information security management.

An information security strategic plan attempts to establish an organization's information security program (Lampson 2004). The information security program is the whole complex collection of activities that support information protection. An information security program involves technology, formal management processes, and the informal culture of an organization. (Byrne 2006) An information security program is about creating effective control mechanisms, and about operating and managing these mechanisms Information security strategies have been defined and classified in a number of different ways and subsequently, there is no widespread agreement on their definition or classification. Studies have identified various strategies such as Deterrence (Patermoster 2010; D'Arcy *et al.* 2009), Prevention Surveillance, Detection (Zimek 2010; Stolfo 2004), Response (Straub, 2011), Deception (Carroll & Grosu 2009).

3.2.1 Prevention

Prevention aims to protect information assets prior to an attack by prohibiting unauthorized access, modification, destruction, or disclosure (Stalling, 2012). Approaching information security strategy from a purely preventive mindset implies that the organization has little tolerance for impact of any kind; therefore counter measures must be deployed with a view to blocking all attacks on the organization. Prevention strategies can be used to avoid information leakage. For example, a clean desk policy enforced by periodic inspections for misplaced and sensitive documents can be useful. From a technical point of view, barriers can be installed around valuable assets prior to an attack (Kankanhalli *et al.* 2003). A commonly used prevention control is authentication, which aims to limit access to authorized users (Lampson 2004; Stalling 2012).

Further prevention techniques include the utilization of software that regulates user interaction with information assets (Peltier 2005; Stalling, 2012), encrypting information flowing over networks to prevent leakage - even if the network is compromised, using firewalls to filter network traffic, and using intrusion detection systems that employ anomaly and signature detection paradigms to identify suspicious data (Zalenski 2002; Stalling 2012).The importance of scanning systems for vulnerabilities, and subsequently patching these vulnerabilities, has been recently highlighted (Spears, 2010). As a result, updating and patching application systems has become a critical preventive technique aimed at denying attackers pathways into the organization. Additionally, vulnerability checking is being used to probe possible or potential weak points in the security infrastructure, aggressively using techniques named "red teaming" or "penetration testing" (Arce & McGraw 2004; Evans *et al.* 2004; Ray *et al.* 2005; Virta 2005).

3.2.2 Deterrence

Deterrence employs disciplinary action to influence human behavior and attitude (Yang, 2013). When applied within organizations, the effectiveness of deterrence is influenced by two key factors – certainty of sanctions and severity of sanctions. The certainty of sanctions (i.e., the probability of being caught) is influenced by the level of awareness of the kind of sanctions, as well as the ability of enforcing bodies to detect offending behavior. The severity of sanctions is influenced by the range of sanctions that can be imposed (Siponen & Vance, 2010). In the west, civilian organizations can only apply security strategies in a defensive capacity. Therefore, deterrence is typically applied internally, targeting company personnel.

Deterrence is effective in guiding employees towards legitimate, acceptable use behavior (Stevens, 2008), in discouraging weakly motivated internal perpetrators (Rao, 2009), in reducing insider abuse and misuse of information systems (Young & Case, 2004), and in influencing employee intentions (D'Arcy *et al.* 2009). The strategy is grounded in criminology and has been widely accepted in the military, international relations, and information warfare (Waterman, 2009).One of the main foci of deterrence is in security policy, where deterrence has been used to specify punishment of employees that fail to adhere to policy statements.

Mahmood (2007) emphasize that organizations should operate an education and training program to inform employees of organizational policy and guidelines in order to make information security efforts more effective. Additionally, Straub (1990) reports that deterrence efforts, such as the severity of penalties, awareness of deterrence actions, and the number of security staff have been successful in the reduction of computer abuse. Others have found that deterrence efforts have a positive effect on information security, although the severity of penalties did not influence effectiveness (Kankanhalli *et al.* 2003). More recently, D'Arcy *et al.* (2009) found that the severity of penalty influenced the amount of abuse in a significant way, which is contrary to Kankanhalli *et al.* (2003)'s outcomes. Siponen and Vance (2010) recommended that organizations should increase training in security policy compliance and should focus on policing policy breaches.

However, Hu *et al.* (2011) identified that deterrence using punishment alone was insufficient in enforcing information security and suggest that organizations reduce the perceived value of information assets. They also state that organizations need to employ high moral standards and self-control (Hu et al. 2011); in essence stating that security culture will influence deterrence efforts. This is in line with recent studies conducted in security culture (DaVeiga & Eloff 2010; Lim *et al.* 2012).

3.2.3 Surveillance

Surveillance is the systematic monitoring of the security environment aimed at developing situational awareness to adapt to fast-changing circumstances and threats (Doyle *et al*. 2009). Situational awareness enables security decision makers to better cope with information security incidents and develop more effective defenses (Bearavolu *et al.* 2003). Monitoring the information security environment of an organization in the physical and digital sphere using technical and non-technical means is challenging. Monitoring of various aspects of an individual's interaction with information and information systems includes logging access to restricted physical and logical spaces where hardcopy and softcopy information is kept.

From a technical point of view surveillance typically uses information generated from strategically placed sensors' augmented with visualization tools to increase security managers' understandability of the situation (Ohno *et al.* 2005; Doyle *et al*. 2009; CSSP 2009). Information collected for surveillance is typically sourced from systems and applications software (Dourish & Redmiles 2002), including intrusion detection systems that report on the number of attacks, degree of attack propagation, and type of attack.

3.2.4 Detection

Detection is an operational-level strategy aimed at identifying specific security behavior (Hamill *et al.* 2005).The objective of detection is to allow the organization to react in a targeted manner. This strategy contrasts with surveillance in that the latter aims to understand the overall situation. Detection therefore, focuses on a specific event whereas surveillance observes the status as a whole.

Detection takes many forms including identification of malicious or unusual behavior (Eilertson *et al.* 2004), intrusion or misuse (Liu *et al.* 2012), and specific attacks against web servers (Debar & Tombini, 2005). Additionally detection can be used to trigger the gathering of evidence of misuse regarding suspicious activity as well as identification of perpetrators (Mahmood, 2007). Various security technologies are used within the detection strategy including dedicated computer and network intrusion detection devices, network scanners, system scanners, misuse and anomaly detectors, content screening and antivirus software, and audit programs (Liu *et al.* 2012; Tapiador & Clark, 2011). To be useful to an organization's security managers, detection of attacks and reporting must be timely and false alarms must be minimized (Hamill et al. 2005). Information provided to security managers stemming from detective measures should ideally be actionable and useful, such as whether an attack has begun, when the attack began, and the scope of the attack (Ray, 2012).

3.2.5 Response

Response takes appropriate corrective actions against identified attacks. The response to an attack can be divided into two phases. Firstly the reaction phase, where appropriate actions are taken against the attacker/attack and secondly the recovery phase, where the situation is restored to its original state (Armstrong *et al*. 2004; Saydjari 2004; Hamill *et al.* 2005). Security managers have considerable tactical options depending on how they want to react to an attack. For instance, a reaction may be to 'exclude' an attacker by transporting them to a different position (Lampson, 2004).

Response could be implemented by dropping a connection, blocking a suspicious IP address at a perimeter firewall or by employing a deception strategy by the use of a honeypot. Another tactic is containment, which separates the attacker and/or attacked area from other (unaffected) areas (Grance *et al.* 2004). Lastly, it is worth noting the literature also discusses offensive responses such as 'strike-back' (Jansen, 2011) and 'strike-first' even though they are not legal options for private organizations in the Western World. In the digital environment, an automated response is particularly important given the relative speed of attack compared to the speed of human decision-making (Williamson 2004). In this situation, a previously designated response to pre-defined conditions of threat, attack, and/or damage can be taken (Cahill, 2003).

3.2.6 Deception

The Deception strategy distracts an attacker's attention from critical information assets using decoys, thereby leading the attacker to waste time and resources (Krutz, 2010). The concept of the deception strategy originates in the military discipline where it is defined as the ability to "enhance, exaggerate, minimize, or distort capabilities and intentions; mask deficiencies; and otherwise cause desired appreciations where conventional military activities and security measures were unable to achieve the desired result" (Krutz &Vine, 2010). Deception has two constructs: passive deception and active deception. Passive deception focuses on hiding something, whereas active deception focuses on showing something (Rice *et al.* 2011).

The techniques of the passive deception include concealment and camouflage; whilst in active deception include false and planted information, ruses, displays, demonstrations, feints and lies (Irvan, 2006). According to Rice *et al.* (2011) and Fowler and Nesbit (1995) there are several principles of effective deception including: reinforcement of the adversary's expectations, realistic timing and duration, and coordination with the concealment of true intentions. These can also be applied in the information security domain. In information security, deception is used to persuade an adversary to believe that false information they were given was actually true, thus driving them towards changing a course of action to what the defender intended, or to expose an attacker to other defensive measures (Rice *et al.* 2011).

Deception has proved effective in misdirecting attackers, even groups of skilled attackers, to a fake, imitation information system where they could be observed without endangering the organizations real systems (Cohen& Koike, 2004). In order to guide an adversary to such a system, a decoy is used to grab the attention of attackers (Tinnel *et al.* 2002). Two types of decoys have been discussed - software decoys and honey pots. A software decoy is wrapper that communicates with calling processes or threads on behalf of critical software (Michael 2002; Michael & Wingfield 2003). When using software decoys, attention may have to be paid regarding the technical misuse since the decoy is implemented with software which is intrinsically vulnerable and imperfect (Michael & Wingfield, 2003). Honey pots are designed to trap unauthorized attackers by convincing them that the system is a real and valuable target to compromise (Rowe 2006; Carroll & Grosu, 2009). A honey pot buys security manager's time while an attacker expends resources to compromise the honeypot (Chakrabarti & Manimaran, 2002).

3.5.7 Perimeter Defense

In the context of information security, perimeter defense involves the creation of a boundary around information assets that is secured by regulating traffic at every incoming and outgoing information channel (choke points) (Schneier, 2006). Network firewalls, access control mechanisms, authentication mechanisms, countermeasures against (distributed) denial of service attacks are typical controls implemented as part of perimeter defense (Shirey, 2007).

According to Song (2005), perimeter defense can be useful for channel monitoring, prohibiting spyware installation, blocking reverse connections, and managing script kiddies. However, if it is the only line of defense then there is no secondary means of defense if it fails (McGuiness 2010). Snyder (2006) suggests that using a perimeter defense strategy may not be optimal as connecting wireless devices to many networks is not difficult, and may expose the organization to other attacks, from the inside. For instance, the CEO uses their computer at home and at the office, and by connecting to the network at the office they may inadvertently begin to propagate malware, via email. This in turn negates the perimeter.

Compartmentalization reduces an attacker's opportunities by dividing the intended area of attack into zones that are secured separately (Schneier, 2006). In this way, an attacker that has overcome the defenses of one zone does not automatically have access to all other zones. Compartmentalization is frequently used in the military to secure information flows. Information is classified into categories such as secret and top-secret. Personnel are assigned clearances that dictate which category of information they can access. This technique can prevent individuals with access to the organization from accessing all information and makes it progressively more difficult to access information of higher classifications. Compartmentalization can also be used to protect networks and computing systems. A typical example of this strategy is a DMZ (De-Militarized Zone) or a network area isolated from the internal network but open to public to allow access from the outside the company (Applegate, 2012). Publicly accessible 'proxy' servers (e.g. for we band database services) are located inside the DMZ to prevent external traffic from directly interacting with trusted internal servers.

3.5.8 Layering

Layering uses multiple countermeasures that function independently, but increases the overall effectiveness of the defense when working together, thereby posing a series of challenges to the attacker. The defensive systemic designed to be resilient by overlapping a series of countermeasures, where each countermeasure complements the next, so that if one fails, another will back it up (Jones 2005; Rubel *et al.* 2005; Price 2010; Byrne 2006; Snyder 2006). The strategy originates from the design of medieval castles that featured concentric walls aimed at slowing down the progress of enemies whilst castle defenders engaged the enemy from towers (Price, 2010).

Layered defense is predicated on the belief that a single strategy is insufficient to handle the attacker's arsenal of sophisticated, intelligent, and innovative technologies (Rosenquist 2008; Gandotra *et al.* 2009; Price 2010). Given the vulnerabilities in the intrinsically complex and imperfect software platforms in organizations, perfect security is impossible (Lampson 2004; Price 2010). However, multiple defensive layers with different sets of vulnerabilities are more difficult to defeat than a single layer and create significant delay which benefits the defending side (Byrne 2006; Gandotra *et al.* 2009).

Attackers consume their resources and time while they are trying to devise ways to overcome the hurdles on their attack path (Debar, 2012), attacks are mitigated and damage to the information assets is minimized (Peterson, 2007). Several studies have shown layered defense to be effective in handling attacks against information assets. Gurtov *et al.* (2013) found that layering increases security. Jackson and Ferris (2013) showed that layered defense is effective in mitigating attacks through three experiments mobilizing "red teams". Stytz (2004) posited that layered defense is cost-effective and more resilient than perimeter defense.

4.0 Conclusion

The study observed that many organizations especially financial players operate in large-scale network environments with numerous servers, fixed terminals and portable wireless devices including laptops and smart phones. In addition, there are employees with complex access profiles to masses of information at varying levels of sensitivity. Devising strategies to contend with risk exposure in financial security environments requires a systematic and comprehensive approach with a view to learning and developing situational awareness especially from security incidents.

Organizations and their information systems constantly change, the activities within the security management process must be revised continuously, in order to stay up-to-date and effective. However, many organizations have put little effort to ensuring proper organizational information security ignoring the strategic importance of information in decision making, if information is utilized well it can generate good basis for decision making. Senior management should have commitment to the security strategy function, and there should be a high-level of involvement in strategizing to enhance the development of security strategy within organizations.

The strategies focused on security management include prevention, deterrence, surveillance, detection, response, deception, perimeter defense and layering. Of importance is the loss prevention which focuses on what critical assets are and how they can be protected. Attacks can be prevented by employing these strategies and the improvement of system efficiency. Secure financial systems can be a completive edge in the market.

5.0 Recommendation

Strategies should be devised to contend with risk exposure in financial security environments which requires a systematic and comprehensive approach with a view to learning and developing situational awareness especially from security incidents. Organizations should increase funding in order to strengthen the security function, this will help the unit avoid any leakage of important which can be a threat to the competitive advantage of the organization.

Prevention, deterrence, surveillance, detection, response, deception, perimeter defense and layering risk management strategies should be appropriately implemented to minimize financial loses. Employees should be trained on how to use the systems in order to enhance efficiency in the organizations. Organization should invest on both human resources and current technology to enhance secure systems and financial integrity.

References

Anderson EE, Choobineha J (2008*) Enterprise information security strategies*. Computers & Security 27:22–29

Anderson P (2001) Deception: *A Healthy Part of Any Defense in-Depth Strategy*. SANS Institute InfoSec Reading Room, February 15, 2001 edn. SANS Institute.

Andres, R. (2012). The Emerging Structure of Strategic Cyber Offense, Cyber Defense, and Cyber Deterrence. *Trans. Array Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World. Derek S. Reveron. 1st ed. Washington DC: Georgetown University Press*.

Applegate, S. D. (2012). The principle of maneuver in cyber operations. In *Cyber Conflict (CYCON), 2012 4th International Conference on* (pp. 1-13). IEEE.

Arce I, McGraw G. (2004) *Why Attacking Systems Is a Good Idea*. IEEE Security & Privacy 2 (4):17-19

Armstrong D, Carter S, Frazier G, Frazier, T. (2004) Autonomic Defense: T*hwarting Automated Attacks via Real-Time Feedback Control*. Complexity 9 (2):41-48

Artail H, Safa H, Sraj M, Kuwatly I, Al-Masri Z (2006) *A Hybrid Honeypot Framework for Improving Intrusion Detection Systems in Protecting Organizational Networks. Computers & Security* 25:274-288

Barford P, Dacier M, Dietterich TG, Fredrikson M, Giffin J, Jajodia S, Jha S, Li J, Liu P, Ning P, Ou X, Song Defense. Cyber Situational Awareness, Advances in Information Security (46):3-13

Baskerville, R., Lyytinen, K., Sambamurthy, V., & Straub, D. (2011). A response to the design-oriented information systems research memorandum. *European journal of information systems*, *20*(1), 11-15.

Baskerville, R., Spagnoletti, P., & Kim, J. (2014). Incident-centered information security: Managing a strategic balance between prevention and response. *Information & Management*, *51*(1), 138-151.

Bauer M (2001) *Designing and Using DMZ* Networks to Protect Internet Servers. Linux Journal 2001 (83)

Bearavolu R, Lakkaraju K, Yurcik W, Raje H (2003) *A Visualization Tool for Situational Awareness of Tactical and Strategic Security Events on Large and Complex Computer Networks*. Paper presented at theMilitary Communications Conference (MILCOM) 2003, 13-6 Oct.

Beckman S., L, Rosenfield D., B. (2008) Operations Strategy: *Competing in the 21st Century. McGraw-Hill/Irwin, New York*

Bowen P, Hash J, Wilson M, Bartol N, Jamaldinian G (2006) *Information Security Handbook: A Guide for Managers*. . NIST Special Publication 800-100. NIST, Gaithersburg, MD.

Brykczynski B, Small RA (2003) *Reducing Internet-Based Intrusions: Effective Security Patch Managemen*t. IEEE Software:50-57

Burnburg MK (2003) *A Proposed Framework for Business Information Security Based on the Concept of Defense-in-Depth. Master's Thesis*, University of Illinois at Springfield, Springfield,

Byrne P (2006) *Application Firewalls in a Defense-in-Depth Design. Network Security* (9):9-11

Cahill TP (2003) *Cyber Warfare Peacekeeping. Paper presented at the* 2003 IEEE Workshop on Information Assurance, Jun.

Cao J, Lin M, Deokar A, Burgoon J.,K, Crews JM, Adkins M. (2004) Computer-Based Training for Deception Detection: What Users Want? ISI 2004, LNCS 3073:163–175

Cao, H., Zhu, P., Lu, X., & Gurtov, A. (2013). A layered encryption mechanism for networked critical infrastructures. *IEEE Network*, *27*(1), 12-18.

Carroll T., E, Grosu D (2009*) A Game Theoretic Investigation of Deception in Network Security. Paper presented at the 18th International Conference on Computer Communications and Networks* (ICCCN '09), Jan

Chakrabarti A, Manimaran G. (2002) *Internet Infrastructure Security*: A Taxonomy. IEEE Network 16 (6):13-21

Chen, S., & Song, Q. (2005). Perimeter-based defense against high bandwidth DDoS attacks. *IEEE Transactions on Parallel and Distributed Systems*, *16*(6), 526-537.

Cohen F, Koike D (2004) Misleading attackers with deception. Paper presented at the Information Assurance Workshop, 2004. Proceedings from the Fifth Annual IEEE SMC, 10-11 June 2004.

CSSP (2009) Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In- Depth Strategies. Control Systems Security Program, National Cyber Security Division, Department of Homeland Security

Strater L, Swarup, V., Tadda, G., Wang C, Yen, J. (2010) Cyber SA: *Situational Awareness for Cyber*.

D'Arcy J, Hovav A, Galletta DF (2009) User Awareness of Security Countermeasures and its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research* 20 (1):79-98

Da Veiga A & Eloff JHP (2010) A framework and assessment instrument for information security culture, *Computers and Security* 29(2):196-207.

Dasgupta D. (2004) Immuno-Inspired Autonomic System for Cyber Defense. *Computer Science Technical Report*. Univ. of Memphis.

Debar H, Morin B, Boissee V, Guerin D (2005) An Infrastructure for Distributed Event Acquisition. Paper presented at the European Institute for Computer Antivirus Research (EICAR) 2005 Conference Best Paper, Saint Julians, Malta, April

.

Dourish P, Redmiles D (2002) An Approach to Usable Security Based on Event Monitoring and Visualization.

Hendriks, C. J. (2013). Integrated Financial Management Information Systems: Guidelines for effective implementation by the public sector of South Africa. *South African Journal of Information Management*, *15*(1), 1-9.

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), 154-165.

Illinois B., S. (2002*) Security Attribute Evaluation Method: A Cost-Benefit Approach. Paper presented at the 24thInternational Conference on Software Engineering* (ICSE '02), New York, NY,

Jackson, S., & Ferris, T. L. (2013). Resilience principles for engineered systems. *Systems Engineering*, *16*(2), 152-164.

Jansen, W. A. (2011). Cloud hooks: Security and privacy issues in cloud computing. In *System Sciences (HICSS), 2011 44th Hawaii International Conference on* (pp. 1-10). IEEE.

Kriegel, H. P., Kröger, P., & Zimek, A. (2010). Outlier detection techniques. *Tutorial at KDD*, *10*.

Krutz, R. L., & Vines, R. D. (2010). *Cloud security: A comprehensive guide to secure cloud computing*. Wiley Publishing.

Paternoster, R. (2010). How much do we really know about criminal deterrence?. *The journal of criminal law and criminology*, 765-824.

Peltier, T. R. (2005). *Information security risk analysis*. CRC press.

Poolsappasit, N., Dewri, R., & Ray, I. (2012). Dynamic security risk management using bayesian attack graphs. *IEEE Transactions on Dependable and Secure Computing*, *9*(1), 61-74.

Rebollo, O., Mellado, D., Fernández-Medina, E., & Mouratidis, H. (2015). Empirical evaluation of a cloud computing information security governance framework. *Information and Software Technology*, *58*, 44-57.

Richardson, R., & Director, C. S. I. (2008). CSI computer crime and security survey. *Computer security institute*, *1*, 1-30.

Rodin-Brown, E. (2008). Integrated financial management information systems: A practical guide. *United States Agency for International Development.*

Rowland, C. H., Pettit, J., Rhodes, A., & Irwin, V. (2006). *U.S. Patent No. 7,058,968*. Washington, DC: U.S. Patent and Trademark Office.

Sabahi, F. (2011). Cloud computing security threats and responses. In *Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on* (pp. 245-249). IEEE.

Schwalbe, K. (2015). *Information technology project management*. Cengage Learning.

Siponen, M., Pahnila, S., & Mahmood, A. (2007). Employees' adherence to information security policies: an empirical study. In *IFIP International Information Security Conference* (pp. 133-144). Springer, Boston, MA.

Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. *MIS quarterly*, 503-522.

Stevens, B. (2008). Corporate ethical codes: Effective instruments for influencing behavior. *Journal of Business Ethics*, *78*(4), 601-609.

Van Niekerk, J. F., & Von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security*, *29*(4), 476-486.

Wailly, A., Lacoste, M., & Debar, H. (2012, September). Vespa: Multi-layered self-protection for cloud resources. In *Proceedings of the 9th international conference on Autonomic computing* (pp. 155-160). ACM.

Whitman, M. E., & Mattord, H. J. (2011). *Principles of information security*. Cengage Learning.

Young, K. S., & Case, C. J. (2004). Internet abuse in the workplace: new trends in risk management. *Cyber Psychology & Behavior*, *7*(1), 105-111.

Zhang, D., Wang, Y., Suh, G. E., & Myers, A. C. (2015). A hardware design language for timing-sensitive information-flow security. *ACM SIGPLAN Notices*, *50*(4), 503-516.