SOCIETY FOR SCIENCE AND EDUCATION
UNITED KINGDOM

TNC TRANSACTIONS ON NETWORKS AND COMMUNICATIONS

VOLUME 6, NO. 5
ISSN: 2054 -7420

A Stratified Cyber Security Vigilance Model: An Augmentation of Risk-Based Information System Security

Abuonji Paul, Rodrigues Anthony, J., George O. Raburu,
School of Informatics and Innovative Systems, Jaramogi Oginga Odinga University of Science and Technology, P. O. Box 210- 40601, Bondo, Kenya.
pabuonji@jooust.ac.ke; tonyr@jooust.ac.ke; graburu@jooust.ac.ke

ABSTRACT

Information system security in the current interconnected environment called the cyber-space is continually getting more sophisticated. All the players involved- governments, corporates, IS security experts and users, both naïve and sophisticated- all grapple with one big problem: how to decide on what level of security is enough for their information system since the amount of security controls applied must be commensurate with the IS assets being protected. In that regard, many organizations adopt risk-based security, in the hope that it would answer the elusive IS security question, but to no avail. Unfortunately, many such organizations still experience numerous breaches to their Information systems and some even realize they have fallen victims to cyber criminals, long after the actual compromise. It is for this reason that this paper presents a novel security model called Stratified Cyber Security Vigilance (SCSV) model that augments the standard risk-based security approach and demonstrates its ability to improve IS security.

Key Words: stratified, cyber, security, vigilance, model, risk-based

1 Introduction

As our lives continue to depend more on computers, our own security lies in their security [1]. Governments, business enterprises, political players, researchers, and many others, all depend on computer based information systems to effectively accomplish their undertakings. Therefore security of data and the systems that store and manipulate these data is of paramount importance to all technologically progressive organizations. [2] defined information system security as the set of measures and mechanisms that are put in place in order to safeguard computer or information system's confidentiality, integrity and availability with the aim of preventing unauthorized disclosure, unauthorized modification and unauthorized withholding. [3] on the other hand defines it as the protection afforded to an automated information system in order to attain applicable objectives of preserving integrity, availability and confidentiality of information system resources. In the current digital age, it is difficult to confine information, data and network software to geographical localities and so can't we confine their security [4]. It therefore means that when conceptualizing, designing and implementing IS security must take global perspective and the mechanisms put in place must consider both stationary and transit data

DOI: 10.14738/tnc.65.5166
Publication Date: 14th September 2018
URL: http://dx.doi.org/10.14738/tnc.65.5166

as well as being cognizant of the complexities and challenges emanating from diverse legal jurisdictions involved. This whole complex process must be done in a risk-based, cost-effective manner [5].

2 Related Works

Risk-based information system security begins by identifying the assets to be protected, calculating their values so that they are neither over protected nor under protected, assessing both internal and external threats to the system, identifying system vulnerabilities and then conducting threat-vulnerability (T-V) paring to determine which threats are likely to exploit which vulnerabilities to harm the system. In this process, the security expert deals with both real and perceived threats [6]. Information system threats and vulnerabilities cover a wide array of events, virtually none of which can be totally eliminated while still operating the system [7].

Since no system can be rendered totally secure, once threats and vulnerabilities are identified, their impact on the total system must be assessed to determine whether to accept the risk of a particular danger, and the extent to which corrective measures can eliminate or reduce its severity. The primary goal for an IS Security professional involves putting efforts to reduce the threat window, which is the time between detection of an incident and response [8]. This is one of the fundamental aspects of creating a robust security program. It therefore means that detection must be prompt and appropriate action taken immediately. For prompt detection to take place there is need to use a security model that delivers high level of vigilance. [9] said that one best practice towards network security is to build the network model in a way that can foster security. And [10] indicated that, lack of attention on the part of management has exposed many information systems to security breaches. These facts elevate the concept of vigilance to the centre stage of an effective information system security program.

Many information system security models have been proposed in attempt to improve security. These models range from specific to general purpose and do sometimes overlap, depending on designers or implementers. Whatever the case, the models should help in achieving the main information security goals namely confidentiality, integrity, availability, authentication and accountability [11]. The system should be secure, both from the user and administrator perspective. [12] explained that secure systems must have been built using secure components such as strong cryptographic algorithms, secure key redistribution mechanisms and robust authentication protocols. Some of these systems include Pretty Good Privacy (PGP) which provides email security and operates at the application layer, Secure Shell (SSH) which provides security during remote system login. At the transport layer are the Secure Socket Layer (SSL) and the newer version called Transport Layer Security (TLS). Finally IPsec protocol operates at the IP or network layer.

Some common security models include access control list, Bell-La Padula model, Biba model, Brewer and Nash model, Capability-based security, Clark-Wilson model, Graham-Denning model, Harrison-Ruzzo-Ullman model and lattice-based access control model. Others are mandatory access control, object-capability model, role-based access control, take-grant protection model and protection ring. Some implement specific aspects of security- for example Bell-La Padula for confidentiality while Biba and Clerk-Wilson models are geared toward safeguarding data integrity. While Bell-La Padula and Biba models approach access control from a static standpoint, the Brewer and Nash model, also called Chinese wall model provides information security access controls that have the capacity to change dynamically. Its

intention was to provide controls that can mitigate conflict of interest in commercial organizations. Most of these models need to be integrated into a more comprehensive and holistic model in order to be able to protect an enterprise end-to-end in line with the organization's security policy [13].

An example of such a model was proposed by [3]. He described a more general and holistic model for network security as shown in figure 1 below. He demonstrated a scenario where the sender intends to transmit a message to the recipient over the internet. Since the internet is inherently insecure by virtue of its pervasive and ubiquitous use, it is expected that some secure mechanism must be put in place to ensure safe communication.

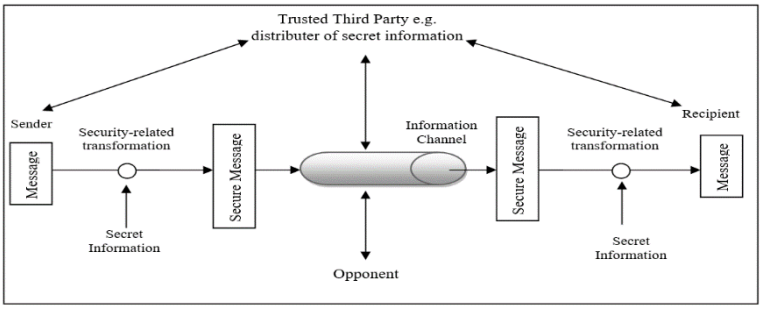

Figure 1: Model for Network Security (Stallings, 2011)

This model borrows heavily from the ideas of [12] explained above. Security related transformation is done using secret information provided by the trusted third parties- in this case encryption keys. This model if adopted and properly implemented can safeguard confidentiality of data through encryption. However it is silent on integrity and availability of data and information systems. Moreover, this paper contends that security in whatever form- whether administrative, physical or logical is miserably impractical without vigilance on the part of security agents, other stakeholders including those being protected and the information system itself.

Generally speaking, vigilance is the process of paying more careful attention, especially in order to notice possible danger [14]. From psychology perspective, vigilance refers to the ability of organisms to maintain their focus of attention and to remain alert to stimuli over prolonged periods of time [15]. In information systems, security of computers or programs largely depends on the efficiency of its vigilance mechanisms that prompts its users and administrators when an abnormal activity occurs [16]. With brisk and widespread adoption of computer systems coupled with quick-fix application development and deployment tendencies, everything in the information system infrastructure appears to be vulnerable. To that end, security of information systems has become a cause of great concern.

In its cyber security report, Deloitte indicated that a good financial system must have three main features- secure, vigilant and resilient. It explained that a secure system must have enhanced risk prioritized controls to protect against known and emerging threats and should comply with industry cyber security standards and regulations. A vigilant system must detect violations and anomalies through better situational awareness across the environment. Finally, a resilient system must establish the ability to quickly return to normal operations and repair any damages to the business [17]. It further illustrates that organizations need multipronged approach to cyber security management involving automated systems and people. This is illustrated in figure 2 below.

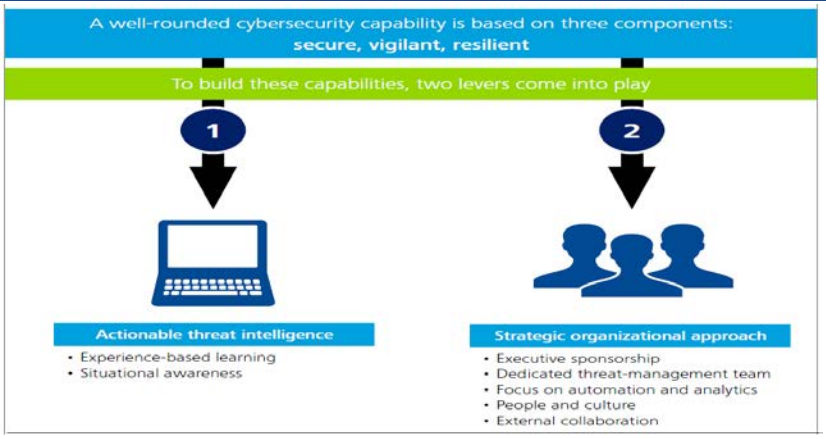

Figure 2: Multipronged Approach to Cyber Security Management
***Source*: Deloitte Center for Financial Services Analysis, Whitepaper (2014)**

Several studies indicate that many cyber-attacks take place against individuals, organizations or states and either go unnoticed or are detected too late thereafter. These attacks are perpetrated either by lone cyber criminals, organized criminals like Anonymous hackers and hacktivists or government agencies. According to [18], United States, British and Chinese governments participate in large scale cyber-crimes in the name of gathering intelligence to curb terrorism or for economic and political espionage. To prevent such acts of law breaking by the supposed law enforcers, citizens ought to be vigilant and defend themselves through civil rights activism or the technology community need to over-engineer their systems to prevent unlawful government surveillance that impinge on citizen's fundamental rights to privacy.

[17] also reported that the response time to cyber-attacks by global financial services firms indicates significant gaps in their preparedness. This is due to inability of these firms to quickly detect and respond to cyber threats. As illustrated in figure 3 below, attack success is the time to compromise the system. It measures time from the first malicious action taken against the victim until the point at which an information asset is negatively affected. Discovery success is the time from compromise of the system to discovery. It measures time from initial compromise to when the victim first learns of the incident. Finally, restoration success is the time from discovery to containment. It measures the time between discovery of a breach to when it is successfully contained. The study showed a big margin between attack success and discovery success, and another big margin between discovery success and restoration success. This clearly shows a lapse in vigilance.

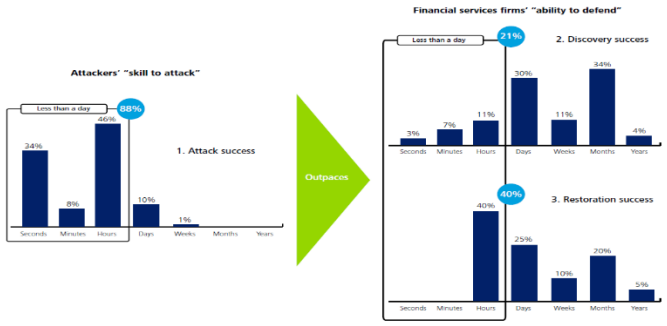

Figure 3: Response time to attacks indicates significant gaps in preparedness
***Source*: Deloitte Center for Financial Services Analysis, Whitepaper (2014)**

The Deloitte study discovered that 34% of successful attacks to information systems happened within seconds; 8% succeed within minutes and 46% succeed within hours. These statistics showed that a whopping total of 88% of information systems that were attacked and got compromised succumbed to their victims within less than a day. Only 10% resisted attacks for days and another 1% for weeks. The remaining 1% was not allocated. This grim state of IS security in financial systems was worsened by the fact that only 21% of targeted organizations had security systems that could detect attacks within a day while majority took longer to detect- 30% took days to detect, 11% took weeks, 34% took months and 4% took years to detect that they were compromised. When it came to restoring the system, no organization was able to restore its system or services within seconds or minutes. The most efficient was discovered to be able to restore within hours, constituting 40%. The other, 25% took days to restore their systems, 10% took weeks, 20% took months and 5% took years to restore their systems. The disturbing results of this study revealed a huge lapse in vigilance and security of information systems in financial services firms.

Kenya's case is not any batter as [19] reported that various sectors of the economy were just coming to terms with the alarming fact that hacking was taking a menacing proportion and causing untold havoc. It stated that in late 2014, companies lost a mindboggling KSh. 15 billion to hackers. The statistics which they got from Kenya Cyber Security Report 2015 showed that an average of 30 companies suffered cyber-attacks in Kenya daily. The bigger problem was that the devastation caused was unlikely to be detected until up to 120 days later. This information showed that there was dire need for enhanced vigilance in order to successfully combat cybercrime.

The necessity for vigilance is usually augmented by the complexity that characterizes information systems security. This is because IS security is pervasive and is a continuous process not an event. A well designed and implemented security program, if forgotten is as good as no security [20]. Besides, vigilance should be stratified to ensure that the degree of vigilance required for any system or resource is commensurate with the level of risk faced by that system or resource. This requires organizations to diligently assess their risk levels and develop a stratified vigilance scheme based on the risk ratings [21].

There is no doubt that risk rating is a principal factor in determining security level of an information system. NIST (2003) defined risk in information systems as the net negative impact of the exercise of a threat on a vulnerability, considering both the probability and the impact of occurrence. Risk management on the other hand is the process of identifying vulnerabilities and threats to the information resources used by an organization in achieving business objectives, and deciding what countermeasures, if any, to take in reducing risk to an acceptable level, based on the value of the information resource to the organization [23].

Risk management is a continuous process that starts by identifying organization's assets or resources that need to be protected and estimating their values; then assessing the threats to those assets or resources, followed by an assessment of all the vulnerabilities that exist in the system. Risk is thereafter calculated based on the probability that a given threat would exploit a vulnerability to cause harm to the systems, and the impact this action would have on the system and business processes. After this determination has been made, the organization needs to identify, select and implement appropriate controls that are proportionate with the level of risk. The final stage is to evaluate effectiveness of the controls and start the process all over again. Note that organizations can take any of the following five possible options when

dealing with risks [24]. They can- mitigate, transfer, accept, avoid or deny the risks. The decision made will depend on the rating of these particular risks, where each risk will be treated individually.

Risks can be calculated or estimated using quantitative or qualitative approaches. In information systems, the most tenable way is using qualitative approach [24]. In this approach, the probability or likelihood of a threat exploiting a vulnerability to cause harm over a period of one year will be rated as low, moderate or high, based on percentages. Table 1 below shows a sample likelihood definition that can be sued.

Table 1: Likelihood Definitions (NIST, 2003)

Ratings	Definition
Low	0-33% chance of successful exercise of threat during a one-year period
Moderate	34-66% chance of successful exercise of threat during a one-year period
High	67-100% chance of successful exercise of threat during a one-year period

On the other hand the level of damage or impact that the attack is likely to exert on the system or business is also rated as low, moderate or high. In many cases this will be evaluated based on the effect on confidentiality, availability and integrity of the information resources of the organization including business processes. Once this is satisfactorily done, the risk determination matrix can be constructed to show how various risks are rated. This is shown in table 2 below.

Table 2: Risk Rating/ Determination Matrix

Impact of the Incidence				
	High	Moderate	High	Very High
	Moderate	Low	Moderate	High
	Low	Very Low	Low	Moderate
		Low	Moderate	High
		Likelihood of Occurrence of Incidence		

As discussed in the previous sections of this research, risk and vigilance are key factors in security of information systems. Even the process of risk management itself requires vigilance. This is because risks and vulnerabilities are dynamic and a vigilant risk management team or system is required to keep pace with the ever changing cyber security landscape (NIST, 2003). A stratified vigilance scheme that matches risk ratings is therefore proposed as follows: very low vigilance, low vigilance, moderate vigilance, high vigilance and hyper vigilance. And using this rating, a risk - vigilance paring for an information system can then be done

This paring helps to provide vigilance which is commensurate with the risk to an information asset. This is supported by Resource Theory of vigilance proposed by [25], [26],[27], [28]. According to this theory, human vigilance depends on the mental capacities or resources that can be allocated to the task. The concept of resources draws on economics of vigilance which supports the assertion that the resources used to secure an asset must be commensurate with the value of that asset. In this case the organizations need to employ both human and automated vigilance which have financial implications.

The concept of vigilance is heavily applied in security [29], [30] and the whole of military spectrum [31]. This study broadly classifies vigilance into two main components namely human vigilance and automated

vigilance. In the modern technology-driven enterprise environments, vigilance has ceased being an exclusive human activity as was the case in the olden days. In addition to involvement of human actors, which is very critical for making semi-structured and unstructured decisions, there are myriad automated systems designed to alleviate the physiological and psychological human resources required in vigilance as an aspect of security.

There are many automated IS devices or components for implementing vigilance. The most commonly used such devices or systems in cyber security vigilance are firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), bandwidth management and monitoring tools, traffic analysis or discovery tools, system alerts, host based scanners, network and port scanners, among others [32], [33].

The other component is human vigilance as earlier stated. One needs to underscore the importance of involvement of human actors in cyber security because automated systems may not have the capacity to make critical unstructured and semi-structured decisions based on environmental and other factors necessary in decision making. For example humans need to view system logs, alerts, alarms and decide how to respond appropriately. There are instances when, one may even decide to shut down the system temporarily in order to solve a more catastrophic attack that would happen if the system remained running throughout. Depending on the organogram of the organization, the human actors may include operational staff, operational level managers or supervisors, middle level managers and top level or strategic level managers [34], [35].

After considering components of vigilance in an IS system, the next thing is to look at vigilance activities in an information system. These are those factors that determine whether a system is vigilant or not but may not necessary be used to measure or rate the quality of vigilance. In psychology, vigilance is described as the ability to maintain concentrated attention over prolonged periods of time with the intention to detect the appearance of a particular target stimulus [36]. The individual watches for a signal stimulus that may occur at an unknown time. This means that vigilant human actors need to constantly observe their environment. To do this, they must be able to detect activities with random occurrences, the stimuli must be transmitted into the brain for interpretation and then an appropriate action or response is made.

[37] recommended the need for a vigilance classification based on the domain of application. When this concept is applied in information system security, vigilance must exhibit similar features to those in psychology, but the components used will be different. The system- both automated and human components- must monitor, detect, interpret, report and respond appropriately to activities and events [38]. The incident or stimulus comes from the environment of the system. This incident is detected by the system, interpreted, reported and a response is made- which in this case should be a corrective action [39].

There are also parameters that can be used to measure the quality of vigilance in an information system. The process of detection, interpretation, reporting and response must be done in a manner that can help in making correct decisions in a timely manner. Consider for example, the British Royal Air Force while using RADAR during the Second World War were not able to detect their targets accurately and hit the German U-boats that were sinking allied ships. Therefore the quality of their vigilance was considered to be poor [40]. For effective and quality vigilance, the indicators of vigilance –detection, interpretation, reporting and response must be done in an accurate and timely manner. Automated and human vigilance components must never issue false alarms. However time for detection, interpretation, reporting and

response can be tampered with the level of risk to the organization. The study therefore finds the need to develop a mechanism to relate risk, vigilance and time constraints allowed for each level of risk to be tackled in compliance with resource theory of vigilance articulated by [41], [42]. In that regard, as the level of risk increases so does vigilance increase and time constraints decrease proportionately. This depicts an inverse relation between risk and time constraints for action. These time constraints can further be matched to the kind of reasonable response that may be required of the system or system administration based on the organization's security policy.

It is worth remembering that vigilance classification is done based on calculated or estimated level of risk to the organization's information system assets. These assets help the organization to pursue its business strategy. From the perspective of strategic management, information technology strategy and its adoption must fit the business strategy since IT should be a driver of business strategy and processes [43]. This means that cyber security risks are not just IT problems but are strategic business problems [17], [10]. Therefore, once information about system risks has been generated, it must be reported for decision making and action. Irrespective of the organogram of the organization, risk must be responded to appropriately and proportionately.

According to [34] in the process of managing different subsystems of an organization, executives at various levels of the organization need to make management decisions. He classifies these decisions as strategic, tactical and operational decisions based on three management levels namely strategic, tactical and operational levels. [44] also classify management levels into three, but with different names- senior management, middle level management and supervisory management. [35] on the other hand describes four levels of management as top management, intermediate management, middle management and supervisory or operational management.

Whichever names given to these levels of management, the single point of agreement is that the top most level of management in any organization deals with the overall strategy of the organization. Middle level deals with interpretation and implementation of the strategy and low level management deals with supervision of the day-to-day operations of his or her section or division in the organization [35], [34]. Figure 4 below illustrates this information.

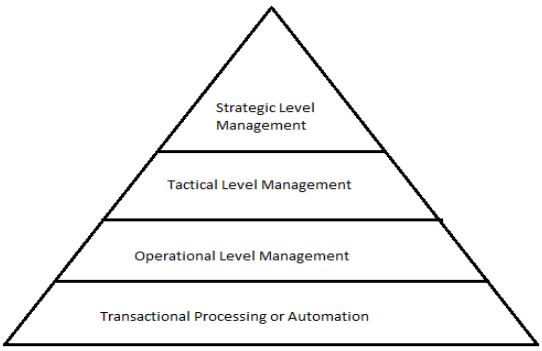

Figure 4: Management Levels (Lucey, 2005)

With reference to the above explanation, highly rated risks have direct impact on the strategic objectives of the organization and therefore should get direct and immediate involvement of the strategic level management of the organization. Moderate risks need the immediate attention of middle level management and low level risks may only need direct and immediate attention of operational level

management. This stratification of response to risk based on management levels is in tandem with economics of risk management and is what partially informs the stratified cyber security vigilance (SCSV) model, developed in the subsequent section.

3 Model Formulation

Proper risk management is the hallmark and foundation for any effective information system security program since organizations need to assess their risks and implement appropriate security controls that can mitigate against those risks [45]. It is for this reason that the study aimed at developing a cyber-security model founded on the widely accepted risk-based information system security model, but with an enhancement called stratified vigilance. As earlier stated, risk management is the process of identifying vulnerabilities in and threats to information resources used by and organization in achieving business objectives and deciding what countermeasures, if any, to take in reducing risk to an acceptable level, based on the value of information resource to the organization [23]. It is as an iterative process comprising of the following steps:

1. Identification of all relevant assets and estimation of their values
2. Conducting threat assessment within the organization and its environment
3. Conducting vulnerability assessment within the organization
4. Performing threat- vulnerability (T-V) pairing
5. Calculating risk in terms of likelihood of occurrence and impact on the information assets
6. Identification, selection and implementation of appropriate security controls
7. Evaluation of the effectiveness of those controls that have been implemented

This process has been illustrated in figure 5 below. It is vital to note that at the center of risk management is business strategy and processes. This is because threats have the potential of disrupting business processes and the overall business strategy of the organization. Therefore risk management process must be owned and driven by the strategic level management. After risk assessment has been conducted successfully, the management of the organization can make any of the following five decisions risk by risk: mitigate the risk internally by implementing appropriate controls or countermeasures; transfer the risk to a third party for example by outsourcing the service or engaging the services of an insurance company; avoid the risk by removing the risky parts of the system being used or replacing it all together with a lower risk system; accept the risk if its likelihood and impact is very low; or deny the risk if it's not clearly articulated.

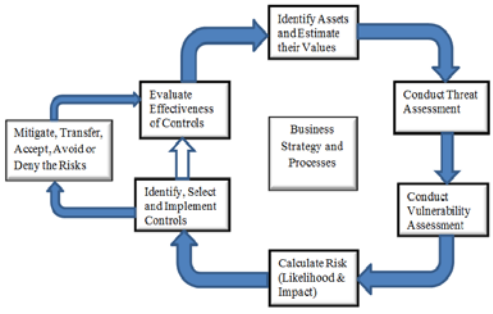

Figure 5: Risk Management Process

Even though risk can be calculated using quantitative or qualitative approach, in information systems risk management, the most tenable approach is using qualitative one [24]. Table 1 and table 2 above

respectively show likelihood definitions and risk rating or risk determination matrix used in qualitative risk management. The five level risk rating scale developed for this study is: very low, low, moderate, high, very high. And as was discussed in previous section risk and vigilance are principal factors in information system security [22], [20], [45]. In the light of this, a stratified vigilance scheme that matches risk ratings would therefore be proposed as follows: very low vigilance, low vigilance, moderate vigilance, high vigilance and hyper vigilance. A risk-vigilance paring for an information system can then be developed as shown in figure 6 below. This rating will help in providing vigilance that is commensurate with risk to an information asset. This is supported by Resource theory of vigilance proposed by [25], [26], [27], [28].

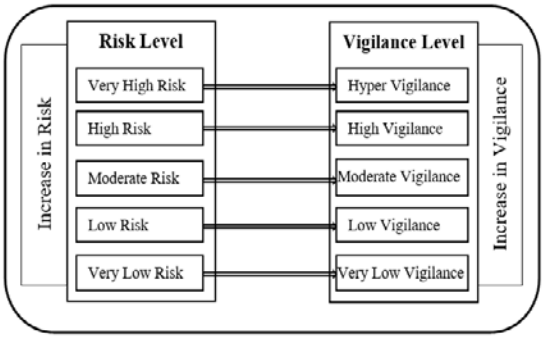

Figure 6: Risk- Vigilance Paring

Once threat - vigilance paring has been done, vigilance needs to be clearly defined in a manner that it can be clearly classified in terms of security roles by human actors [29], [30], [31] and automated technical controls [32], [33]. Additionally, [37] recommended that vigilance should be classified based on the domain of application. Therefore when vigilance is applied in the discipline of information system security, the entire system comprising of automated and human components must be able to monitor, detect, interpret, report and respond appropriately to events and actions [38].

Figure 7 below illustrates this process. The incident or stimulus comes from the environment of the system. This incident is detected by the system, interpreted, reported and a response is made- which in this case is referred to as corrective action. Note that interpretation appears twice. If the information system tools used to implement security vigilance are intelligent then interpretation of security reports are automated. In that case, response to the undesired incident can also be automated. However if the system is not intelligent enough to interpret the incidences correctly then the role is transferred to human actors who will interpret the incident reports and respond to them appropriately. In such as case, then the role of automated security of the information system will simply be to detect and report incidents in raw form for human actors to interpret and respond.

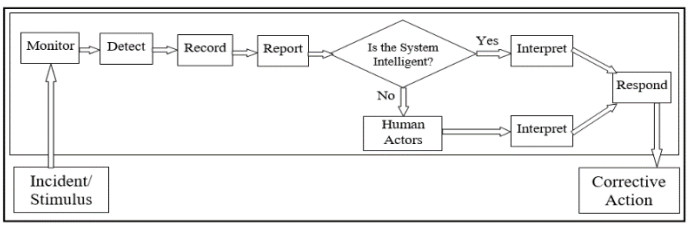

Figure 7: Ideal Information System Security Activities

The quality of vigilance in an information system can be measured in terms of accuracy and timeliness. This means that the process of detection, interpretation, reporting and response must be done in a manner that can help in making correct decisions within an acceptable time constraint. This gives an impression of good quality of vigilance [40]. Figure 8 below illustrates how the stratified vigilance model correlates risk to vigilance in terms of time constraints allowed for each level of risk. Note that as the level of risk increases so does the vigilance increase and time constraints decrease. This depicts an inverse relation between risk and time constraint for action.

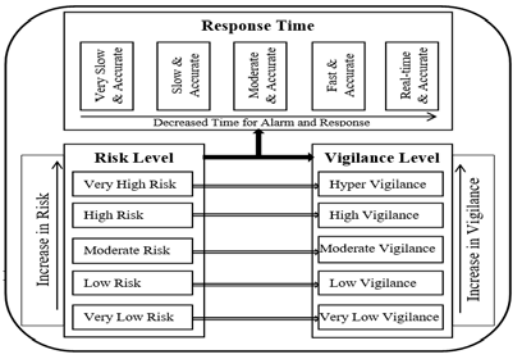

Figure 8: Relating Risk, Vigilance and Time Constraints for Actions

The time constraints described in figure 8 can further be matched to the kind of reasonable response that may be required of system administration based on the organization's security policy. Table 3 below illustrates an example of the possible activities expected of system administration at different levels of vigilance.

Table 3: Time Constrain Metrics for Vigilance

Vigilance Level	System Administration Activities
Very Low Vigilance	System is setup but unmonitored. Owners are content with its existence.
Low Vigilance	System is monitored to ascertain system health.
Moderate Vigilance	If there is a problem, system diagnosis is done to identify cause.
High Vigilance	Ensures that a solution is found and test its effectiveness.
Hyper Vigilance	If no concrete solution is found, propose a solution and escalate.

Since vigilance classification is done based on calculated level of risk, and cyber security risks are strategic business risks [10], [17] therefore risk management is a strategic management role and all other levels of management must perform their respective delegated roles in tandem with that fact [43]. Meaning the entire process must be steered by strategic level management as illustrated in figure 4 above. All these components are then put together to form the SCSV model shown in figure 9 below.

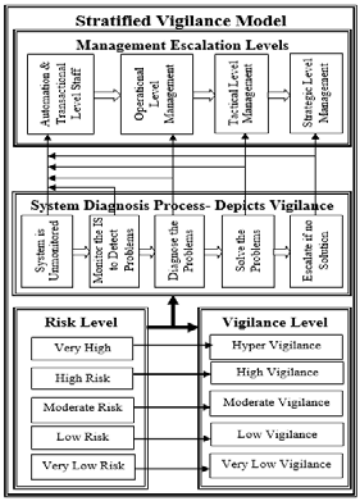

Figure 9: SCSV Model

Five goals of securing information systems and services running in a network have been identifies in this study as the need to identify and control logical threats; the need to identify and control logical vulnerabilities; the need to enhance availability of the system and outsourced services; the need to optimize the utilization of IS resources; and finally the need to produce a proper design and appropriately reengineer the information systems. These goals were also identified as the parameters with which the effectiveness of the SCSV model shall be tested. Appropriate IS design and reengineering is placed at the centre of all the other four parameters since it directly affects other parameters. Figure 10 below illustrates these goals and relates them to ideal information system security activities illustrated in figure 7. These are the activities that are expected to take place in a secure vigilant system. And consequently, figure 10 is a simplification of what a vigilant system is, combined with the parameters identified for testing the SCSV model.

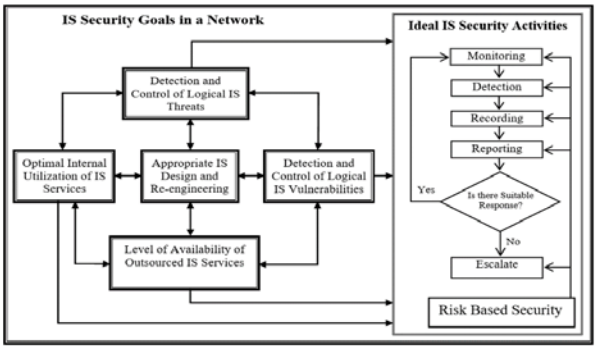

Figure 10: IS Security Goals in a Network and Ideal IS Security Activities

The formulated stratified cyber security vigilance (SCSV) model was then tested using these parameters to validate its effectiveness in mitigating risks in a corporate information system environment. The complete model together with the testing parameters is illustrated in figure 11 below.

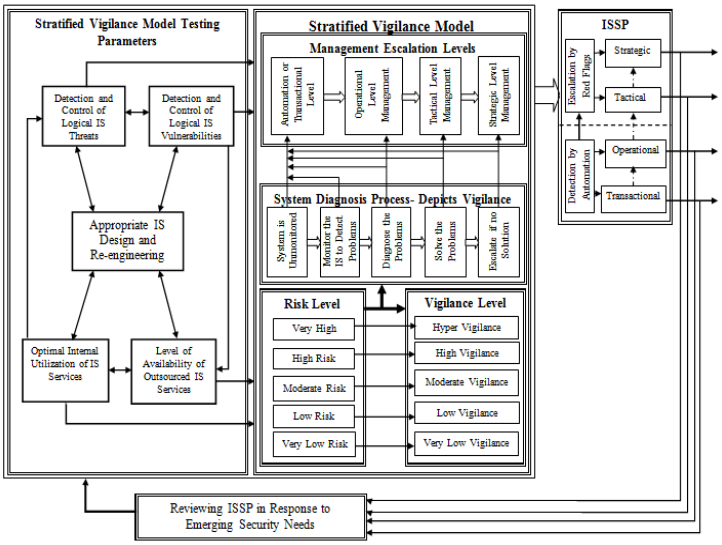

Figure 11: SCSV Model with Testing Parameters

In this model, risks are rated and assigned appropriate levels of vigilance. These levels of vigilance determine who first acts on the risk and how they need to respond. For instance, when a very low level risk is detected in the information system, automated vigilance systems and operational level employees are expected to deal with it conclusively. In case of a medium level risk, the automated systems and operational level managers are expected to report this to tactical level management and they handle it together. If the risk is high, this must be escalated quickly from operational managers, to tactical level managers for appropriate response. However in case of a very high risk, a real-time reporting and escalation is required all the way to strategic level managers. They will then make a decision and recommend actions commensurate with the risk, which may even include reviewing the ISSP. The reporting and escalation can be done using secure emails, SMS alerts, red flags and other forms of alarms depending on response time constraints allowed for each risk level.

4 Model Testing

Preceded by fastidious preparations and meticulous planning, the study entailed designing a sophisticated network infrastructure and deploying various security tools on this network to collect real-time and residual data. The systems were then adjusted appropriately from time to time and at each stage data was collected. Five phases of the system were deployed and tested. Each phase had different configuration and components were set up in a manner that the initial system was simpler in design, configuration and had fewer components while each subsequent phase got more complex in all the above mentioned aspects. Each added level of sophistication represented an advanced level of vigilance. Therefore each of the five levels of system design corresponded to each stratum of vigilance in the model, and this in turn corresponded to each stage of the system diagnostics ability. As illustrated in figure 12 below, the SCSV model was applied in a network to test whether it can improved the system's ability to detect and control logical threats such as computer viruses.

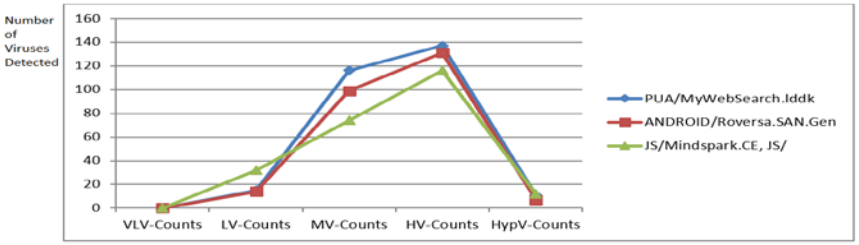

Figure 12: Effect of Vigilance of Virus Detection as Control

The data in figure 12 shows that at very low vigilance level, no viruses were detected because there were no monitoring tools deployed on the network. As the level of vigilance increased, the number of detections steadily increased from low, medium to high vigilance where the highest number of viruses were detected. However, at hyper vigilance level, we observed a sharp decline in the numbers of viruses detected in the system since most viruses have were detected and locked at high vigilance level. However, the remaining viruses needed human intervention to control them such as deployment of other additional controls that could specifically control these viruses.

The SCSV model was also applied on the network to detect and control vulnerabilities. One of the most common logical vulnerability in information systems is unprotected network ports on hosts. A scan was performed on the network and the results shown in figure 13 below were obtained.

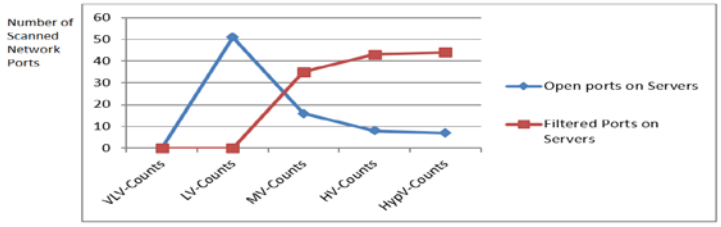

Figure 13: Effect of Vigilance on Status of Communication Ports

As depicted in figure 13 above, low levels of network vigilance was characterized by high numbers of unused open ports on servers while as vigilance increased, most of these ports were filtered using firewall rules thereby increasing the security of servers.

The SCSV model was similarly applied on the network to test stability of two ISP links and results illustrated in figure 14 below.

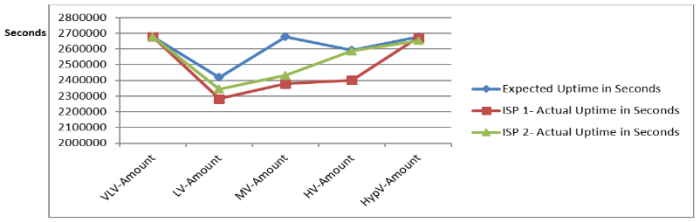

Figure 14: Effect of Vigilance on Link Stability

As depicted in figure 14, from the onset during very low vigilance, no monitoring tools were used and therefore the assumption was that the uptime was the maximum available number of second in a month. However as the level of vigilance increased, it was detected that the uptime for both links wasn't as expected since there were brief, and sometimes prolonged downtimes from time to time. This discovery was followed by timely communication between the organization receiving the service and the ISPs to

ensure prompt restoration of service. It therefore led to better levels of stability for both links as indicated in the graph above.

Finally, we also applied SCSV model in managing access to YouTube which was one of the resources in the internet whose access consumed the highest amount of bandwidth of the organization where the research was done.

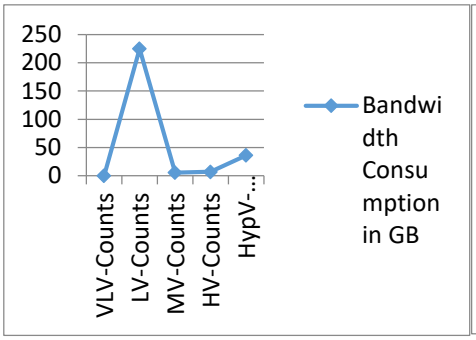

Figure 15 (a): YouTube Bandwidth Usage

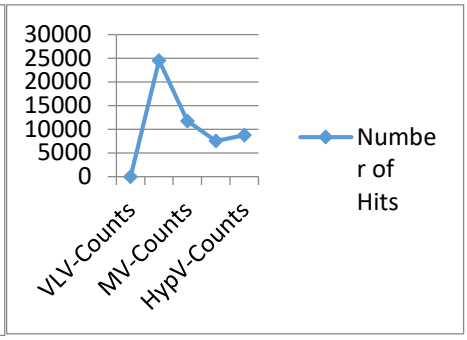

Figure 15 (b): Number of Hits on YouTube

As shown in figures 15 (a) and (b) above, during very low vigilance, no records on YouTube usage were captured because there were no network monitoring tools. However at low vigilance level, the system was configure to monitor the applications running on the network and it detected that about 220 GB of data was being consumed by YouTube alone. A QoS policy was written to control this activity. This resulted into a sharp decline in the amount of bandwidth used in the YouTube steaming to less than 10 GB. After a while the consumption started increasing gradually to about 30 GB. This was as result of users discovering that they had been restricted from accessing YouTube videos and starting to deploy tools to help them circumvent these policies. Table 4 below displays some of the tools users deployed to circumvent the QoS policy restricting the use of YouTube in the network. Figure 15 (b) on the other hand shows that the amount of hits on YouTube declined but not by the same proportion as the amount bandwidth consumed. This was because users continued trying to access the service even when it had been restricted. However when they discovered that they could not access it, most of them gave up but a few decided to use software tools to counter the controls. This majorly happened in subnets 192.168.2.0/24 and to a less extent in subnet 192.168.0.0/24.

Table 4: Tools used to Circumvent QoS Policy in the Network

Tool used to Circumvent QoS Policy	Number of Users in 192.168.2.0/24	Number of Users in 192.168.0.0/24	Number of Users in 192.168.1.0/24
Gbridge VPN Proxy	1069	134	17
Tor Proxy	88	29	5
Ultrasurf Proxy	1025	463	98
Operamini Proxy	2231	74	13
Hotspotshield Proxy	22014	1267	21
Secure Socket Layer Protocol	141702	113221	124619

5 Conclusion

In this paper, we clearly described how we systematically developed and tested the SCSV model for corporate information system security. From the empirical data we collected in-situ, analyzed and used

to test the model, we demonstrated that using the SCSV model in a corporate network would improve the process of detecting and controlling logical threats and vulnerabilities, enhancing optimal utilization of internet bandwidth and increasing availability of internet bandwidth in an organization due to enhanced link stability.

REFERENCES

[1] Goyal, A. (2011), Systems Analysis and Design. Asoke K. Ghosh, PHI Learning Private Limited: New Delhi

[2] Banday, T. M. (2011). Effectiveness and Limitations of E-mail Security Protocols; International Journal of Distributed and Parallel Systems (IJDPS) Vol.2, No.3, May 2011

[3] Stallings, W. (2011). Network Security Essentials: Applications and Standards, 4th Ed; Pearson Education, Inc: Prentice Hall

[4] Tanenbaum, A. S. & Steen, M. V. (2014), Distributed Systems: Principles and Paradigms, 2nd ed. Edinburg Gate: Pearson Education Limited.

[5] Dean, M. (2008). A risk-based approach to planning and implementing an information security program. Paper presented at PMI® Global Congress 2008—EMEA, St. Julian's, Malta. Newtown Square, PA: Project Management Institute.

[6] Wurzler, J. (2013), Information Risks & Risk Management; SANS Institute InfoSec Reading Room. Retrieved on 2-1-2016 from: http://www.sans.org/reading-room

[7] Tanenbaum, A. S. (2011). Computer Networks; 4th ed. Prentice-Hall, Inc: New Jersey

[8] Reck, R. (2014), CISO Spotlight: Robb Reck on Security Strategies for Financial Services. Retrieved on 31-12-2015 from: http://darkmatters.norsecorp.com/2014/12/10/cisospotlight- robb-reck-on-security-strategies-for-financial-services

[9] Habraken, J. & Hayden, M. (2009), Teach Yourself Networking in 24 Hours, 3rd ed. Sams Publishing: United States.

[10] O'Brien, J. A. & Marakas, G. M. (2011). Management Information Systems, 10th ed. McGrow-Hill/ Irwin: New York

[11] Laudon, K. C. & Laudon, J. P. (2012). Management Information Systems: Managing the Digital Firm, 12th ed. Pearson Education Limited: Edinburgh Gate, Harlow.

[12] Peterson, L. L. & Davie, B. S. (2007). Computer Networks: A systems Approach, 4th ed. Elsevier, Inc.: San Francisco.

[13] Sinha, P. K. (2007). Distributed Operating Systems: Concepts and Design. Asoke K. Ghosh, PHI Learning Private Limited: New Delhi.

[14] Cambridge Advanced Learner's Dictionary (2010), 3rd ed. Cambridge: Cambridge University Press.

[15] Parasuraman, R. (1986). Vigilance, monitoring and search. In K. R. Boff, L. Kaufman, & J. P. Thomas (Eds.), *Handbook of human perception and performance: Vol. II. Cognitive processes and performance* (pp. 41-1–41-49). New York: Wiley.

[16] Pandey, S. K. (2012), Security Vigilance System Through Level Driven Security Maturity Model; *International Journal of Computer Science, Engineering and Information Technology (IJCSEIT), Vol.2, No.2*.

[17] Deloitte whitepaper (2014), Transforming cyber security in the Financial Services Industry New approaches for an evolving threat landscape; retrieved on 17th May, 2016, from *www2.deloitte.com/content/dam/.../ZA_Transforming_Cybersecurity_05122014.pdf*

[18] Greenwald, G. (2014), No Place to Hide: Edward Snowden, the NSA & the Surveillance State; Penguin Random House, UK.

[19] Daily Nation Newspaper (23rd November, 2016), Rising Threat of Cyber-attacks Put Companies on the Edge. Published on Tuesday 23rd November, 2016.

[20] Stewart, J. M., Tittel, E. & Chapple, M. (2005), CISSP: Certified Information Systems Security Professional Study Guide; 3rd ed. Sybex Inc.: London

[21] Ward, J. & Peppard, J. (2002), Strategic Planning for Information Systems, 3rd Ed. John Wiley & Sons Ltd: Cranfield, Bedfordshire.

[22] National Institute of Standards and Technology –NIST (2003), Building an Information Technology Security Awareness and Training Program; *NIST Special Publication 800 50. Retrieved on 13th November, 2015 from:* csrc.nist.gov/publications/drafts/800-16-rev1/draft_sp800_16_rev1_2nd-draft.pdf

[23] CISA Review Manual (2016), Certified Information Systems Auditor (CISA) Review Manual 2016. Retrieved on 2nd June, 2016 *from* https://www.isaca.org/bookstore/.../Bookstore-2016-Audit-Catalog_bro_eng_1215.pd.

[24] Elky, S. (2006), An Introduction to Information System Risk Management; SANS Institute Engineering with DiffServ and MPLS Support: *Proceedings of the 15th International Conference on Telecommunications - ICT, St. Petersburg, Russia, 2008a.*

[25] Moray, N. (1967). Where is capacity limited? A survey and a model. *Acta Psychologica*, *27*, 84-92.

[26] Kahneman, D. (1973). *Attention and effort*. Englewood Cliffs, NJ: Prentice Hall.

[27] Norman, D., & Bobrow, D. (1975). On data-limited and resource-limited processing. *Journal of Cognitive Psychology*, *7*, 44-60.

[28] Navon, D., & Gopher, D. (1979). On the economy of the human information processing system. *Psychological Review*, *86*, 214-255.

[29] Hancock, P. A., and S. G. Hart. (2002). "Defeating Terrorism: What Can Human Factors/Ergonomics Offer?" Ergonomics in Design 10: 6–16.

[30] Hancock, P. A., and J. L. Szalma. 2003. "Vigilance and the Price of Freedom." Gateway: Human Systems Information Analysis Center 13 (5): 20.

[31] Lieberman, H. R., Castellani, J. W. &Young, A. J. (2009). "Cognitive Function and Mood during Acute Cold Stress after Extended Military Training and Recovery." Aviation, Space, and Environmental Medicine 80 (7): 629–636.

[32] Awodele, O., Onuiri, E. E. & Okolie, S. O. (2012), Vulnerabilities in Network Infrastructures and Prevention/ Containment Measures: Proceedings of Informing Science & IT Education Conference (InSITE) 2012.

[33] Abdulganiyu, A. (2012), Managing Micro-computer Systems Vulnerabilities in an Institutional Network – The Case of IBB University, Lapai, Nigeria. *International Journal of Information and Communication Technology Research; Volume 2 No. 3: 227- 234.*

[34] Panneerselvam, R. (2009), Production and Operations Management, 2nd ed. New Delhi: Asoke K. Ghosh. page. 3.

[35] Saleemi, M. A. (2013), Principles and Prectices of Management simplified; Nairobi: Printing Services Ltd page 14, 19.

[36] Parasuraman, R. (1986). Vigilance, monitoring and search. In K. R. Boff, L. Kaufman, & J. P. Thomas (Eds.), *Handbook of human perception and performance: Vol. II. Cognitive processes and performance* (pp. 41-1–41-49). New York: Wiley.

[37] Donald, F. M. (2008): The classification of vigilance tasks in the real world, Ergonomics, 51:11, 1643-1655.

[38] Beigh, B. M. & Peer, M. A. (2012), Intrusion Detection and Prevention System: Classification and Quick Review. *ARPN Journal of Science and Technology*, Vol. 2, No. 7, Pp. 661 - 675

[39] Tanenbaum, A. S. & Steen, M. V. (2014), Distributed Systems: Principles and Paradigms, 2nd ed. Edinburg Gate: Pearson Education Limited.

[40] Hancock, P. A. 2013. "In Search of Vigilance: The Problem of Iatrogenically Created Psychological Phenomenon." American Psychologist 68: 97–109.

[41] Navon, D., & Gopher, D. (1979). On the economy of the human information processing system. *Psychological Review*, *86*, 214-255.

[42] Norman, D., & Bobrow, D. (1975). On data-limited and resource-limited processing. *Journal of Cognitive Psychology*, *7*, 44-60.

[43] Lucey, T. (2005). Management Information Systems, 9th ed. BookPower: Hampshire

[44] Rue, L. W., Ibrahim, N. A. & Byars, L. L. (2013), Management Skills and Application, 4th ed.New York: McGraw-Hill Companies Inc page 5.

[45] Ward, J. & Peppard, J. (2002), Strategic Planning for Information Systems, 3rd Ed. John Wiley & Sons Ltd: Cranfield, Bedfordshire.