Modelling of Risk Management Procedures for Cybercrime Control Systems

Alese B. Kayode, Gabriel J. Arome, Olukayode Oluwatoyin and Daramola O.A.

***Abstract*--- This paper proposes formal models for Risk Management Procedures in cybercrime control systems. Mathematical techniques used stem from probability theory, set theory, statistics, and stochastic process theory.**

Index Terms --- Risk Management, Cyberspace, cybercrime

I. INTRODUCTION

Risk Management basically has to do with bearing in mind the possibility that future occurrences may cause adverse effects.

Most modern businesses rely on Information Technology (IT) infrastructure, the security of such infrastructure has today become the major concern spreading across all communities [1].

Cyber space or networks are based on people's interaction. This interaction is based on internet which accelerates dissemination of information and data.

Gereke [2] reported an explosive growth in the number of Internet users over in the last three decades. This is probably due to the development of cheap hardware and wireless access.

Although, the Internet (computer and its networks) is intended for noble works like research and information transfer, some bad elements (individuals) are interested in using it for negative activities. These individuals are often referred to as cyber criminals or hackers.

Information and data exchange via the internet causes computer users to become vulnerable to intruders (hackers), this made computer users very conscious of cybercrime or cyber-attack. Cybercrime is an illegal act of computer experts called hackers, who gain access to a computer system or data belonging to an individual or organization. Many hackers are mere "copycats", not very innovative. They access any number of hacker websites to download malicious code (malware) developed by programmers [3], which attacks and causes dangerous damage to cyberspace.

Manuscript received August 29, 2013. Revised on October 11, 2013

B. K. Alese is with the Computer Science Department of The Federal University of Technology, P.M.B. 704, Akure, Ondo State Nigeria. Phone: +2348034540465; e-mail: kaalfad@yahoo.com.

A. J. Gabriel is with Computer Science Department of The Federal University of Technology, P.M.B. 704, Akure, Ondo State Nigeria. Phone: +2348068991644; e-mail: aromaforgod@yahoo.com

O. Olukayode is with the Computer Science Department of The Federal University of Technology, Akure, Ondo State, Nigeria.

O.A. Daramola is with the Computer Science Department of The Federal University of Technology, Akure, Ondo State, Nigeria.

The Cyberspace is an imaginary environment where electronic data resides. The body of technology which process and practice designs to protect cyberspace from attack, damage or unauthorized access is called cyber security. The International Telecommunication Union (ITU) published a guide for developing countries in 2009. It states that, "developing countries have a unique opportunity to integrate security measures, this may require greater upfront investments, but the integration of security measures at a later point may prove more expensive in the long run" [2].

ITU report suggested that developing countries are exposed to more associated cyber security risks due to their weak protection measures, less strict safeguards and protection [2].

Risk Management is fundamentally concerned with all that could go wrong, and then, decide on ways to prevent or minimize these potential problems. As shown in fig. 1, risk represent an interaction between a hazard that has potential to do some damage, a community that may be damaged and an environment that may be confronted with a serious hazard, or in other circumstances, less serious in order to produce a given consequence.

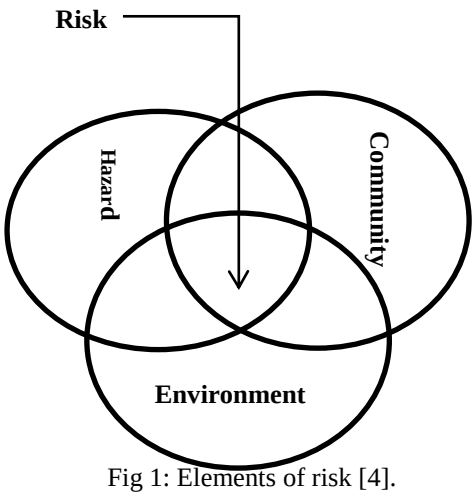

Fig 1: Elements of risk [4].

Risk Management in cyber security control systems can be done by taking some safety measures such as risk assessment, risk mitigation and evaluation of the risk assessment procedures. It is best practice for an organization to apply the same degree of importance to risk assessment on information asset as it would, to financial or operational risk. Cyber security risk, as with all risks, cannot be completely eliminated, but, instead, must be managed through informed decision making processes.

ISBN: 978-988-19252-7-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

Risk management is analogically described as every attempt of crossing a street; oncoming traffic, waiting for the light to change, and using crosswalk.

Also, the ability to analyze the consequences of each decision is risk assessment. Decision taken after performing that quick analysis is risk mitigation based on early proper training and experience of crossing a road. The decision could be, waiting for the traffic light and use the cross walk which greatly reduces the potential risk, or getting a person to make decision(s) by following the person across the street, or simply choose not to cross the street. These decisions are as a result of risk assessment of the situation. If making it across the street is successful, but something went wrong such as a honked horn or brakes squealing, evaluations should be made if another choice would have been better.

Risk management systems help to identify cyber threats (such as viruses, worms, Trojan horses, malware etc.) and design a technique of limiting cybercrime. Cybercrime are usually governed at the national level by law Enforcement Agencies such as Police and cyber threat are monitored by Computer Emergency response Team (CERT) and this risk could also be managed by enforcing some safety measures like policing the network perimeter, installing firewalls and preventing malicious content.

Development of risk management system for cyber security is aimed at enhancing techniques for identifying cyber threats and analyzing monitoring strategies in order to eliminate and guide assets from attacks.

II. MOTIVATION / REVIEW OF RELATED WORKS

There are inherent risks involved in containing and transferring information. Information is subject to intentional and unintentional actions by other people or systems. If information is confidential, there may be unauthorized people who want to access it, such as competitors and disgruntled or curious employees.

People may try to break into the devices containing information or try to intercept the information during transfer. People may also receive confidential information unknowingly and completely by accident. Furthermore, information systems can be maliciously or accidentally damaged. Information security breaches like these can seriously hurt an organization. There is therefore, every need for a risk management system that will enable organizations to frame risk that is; establish the context for risk-based decisions, assess risk, respond to risk once determined, and monitor risk on an ongoing basis, using effective organizational communications and an iterative feedback loop for continuous improvement in the risk-related activities of such organization. This forms the major impetus for this work.

Although, several research works on cyber security have been going on for many years now, none of the related research works have used formal methods to comprehensively identify the risk involved and show how to manage (assessment, mitigation and evaluation) the risks in cyberspace and chart a way forward. In [5], a factor analytical approach was used for carrying out a study on the prevalence of cybercrime in Nigeria. [1] is another related work that explains the extended cost-benefit analysis frameworks designed for international cooperation in cyber security domain, this research only assembles cost and benefit elements; all of which are closely related to the domain of international cooperation in cyber security and utilize cost-benefit analysis as main analysis tool to assess the effectiveness of their targeting policy or business decisions.

Cybercrime and Security Survey Report [6], is also a related work that carried out a survey of cybercrime in Australia. This survey was towards contributing a clearer picture of the cybercrime and security environment in Australia. More so, Mark's survey was limited to Australia which does not have a basic approach of risk management in cyber security. There is every need for comprehensive identification and management of cyber-risks.

The specific objective of this work therefore is to model the Risk Management Processes for cybercrime control systems with a view to providing effective network security management and threat awareness creation.

III. FORMALISATION OF THE RISK MANAGEMENT PROCESS (RMP)

Risk management is an iterative and continuous process, constantly reformed by changing risk landscape, as well as organizational priorities and functional changes.

A well-structured RMP, when used effectively, can help assess risk, and make the best decision based on the information at hand.

Risk assessment allows managers to evaluate what needs to be protected relative to operational needs and financial resources. For instance, organizations accepting online payments are exposed to more risk than websites with only static information.

RMP involves three steps, namely:

A. Risk Assessment

B. Risk Mitigation

C. Evaluation

In developing a consistent framework for analyzing risk management in cyber security, use of questionnaire or other feedback/assessment mechanisms may be required. Fig. 2 is a Risk Management framework showing a summary of the three stages in the RMP.

(A) RISK ASSESSMENT

Risk assessment is the first phase in RMP. Risk is assessed by identifying threats and vulnerabilities, and then determining the likelihood and impact of each risk. This involves periodic review of information security risk with respect to organizational mission/objective. A thorough understanding of the business program component of cyber/information assets (CIA), the technology involved, and the impact as well as the costs of managing the risk are also required.

ISBN: 978-988-19252-7-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

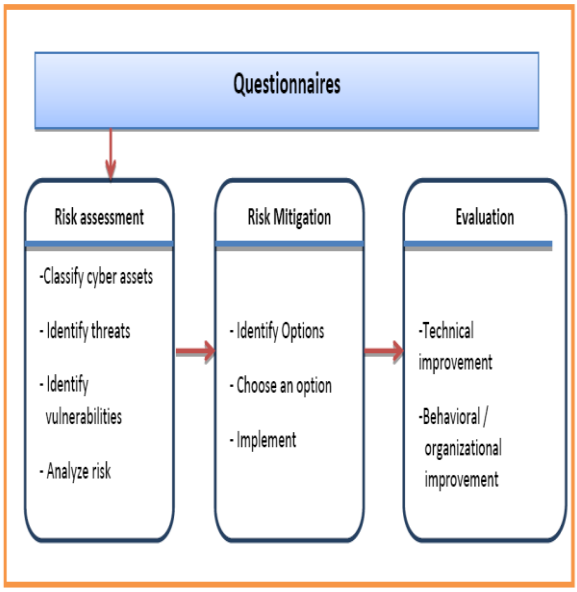

Fig 2: Risk Management Framework

Risk assessments are carried out in the following steps:

A. Classify Cyber/information Asset (CIA)
B. Identify Threat
C. Identify Vulnerabilities
D. Analysis of Risk to cyber/information Assets.

(i) CLASSIFICATION OF INFORMATION ASSETS

Before an organization can assess risk, it must first classify the Information Assets in the organization.

Classifying cyber assets helps dictate the rigor with which they need to be protected by security controls. Information assets can be classified into:

- *Private Information*

Disclosure of information in this category carries a strong possibility of undermining the organization's business mission or security posture. Examples of information in this category may include; Security configuration information, Password, employees' profile.

- *Restricted Information*

In this category, information is public but restricted to some people, and its release has the potential of having negative consequences on the organization's business mission or security posture.

- *Public Information*

Under this category, information is in the public domain and does not require any special protection. An example may be the address and phone number of the headquarters of the organization, which is likely to be made public.

(ii) THREATS IDENTIFICATION

Threats which include, but are not limited to virus, pharming, and denial of service, can be assessed in terms of the probability of an attack. It is important to be aware of threats to an organization's information in order to prevent compromise to that information's confidentiality, integrity and availability. (CIA)

(iii) IDENTIFICATION OF VULNERABILITIES

Vulnerabilities are weaknesses, in a system or facility holding information, which can be exploited to gain access or violate system integrity. Vulnerabilities can be assessed in terms of the means by which the attack would be successful that is, the assess point.

(iv) ANALYZE RISK TO INFORMATION ASSETS

The risk level of an asset is directly proportional to the probability of that asset being attacked. This means, if an asset has a high probability of being attacked then, the risk level of such asset is equivalently be high. If on the other hand, there is a low or no chance of an asset being attacked, the risk level of such asset is very low or even zero.

Since information assets within an organization most likely hold some level of value, risk management will involve reducing the likelihood of threats from occurring. Risk for a given asset can be provided in the most general form as *probability of a threat occurring against an asset multiplied by the value placed on that asset.*

Adopting the probability function and set theory, the set of likely threats *S*, is formalized as;

$$S = \{t_1, t_2, t_3, \dots, t_n\} \quad (1)$$

Where, *t* represents individual threats to the security of the system.

Accordingly, the set of assets *c*, available to the organization is captured as;

$$c = \{a_1, a_2, a_3, \dots, a_n\} \quad (2)$$

Where *a*, represents individual assets.

The probability of a threat on an asset occurring is thus given as;

$$P(t_i) = \frac{\text{no of } t_i \text{ occurrence}}{\text{total no of population}} \quad (3)$$

Or

$$P(t_i) = \frac{\text{number of possible threats}}{\text{total number of assets}} \quad (4)$$

The Risk level, β, on an asset is given as;

$$\beta = P(t_i) * V(a_i) \quad (5)$$

Where, $V(a_i)$ represents the value placed on that asset. The range of this value is as shown below;

$$\{V(a_1) \subseteq [1:3]\}$$

Now, the major objective of Risk Assessment is to get the level of the risk involved. This will help in the decision on how to mitigate such risk/threat/vulnerability. The risk level function, $L(\beta)$, shown below, is for determining whether the level of the risk involved is *high*, *medium*, or *low*.

$$L(\beta) = \begin{cases} \text{High}, & 3 \geq \beta \geq 2.0 \\ \text{Medium}, & 1.9 \geq \beta \geq 0.5 \\ \text{Low}, & \beta \leq 0.4 \end{cases} \quad (6)$$

ISBN: 978-988-19252-7-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

This means, the risk level, β, on an asset is said to be high, if its value ranges from 2 to 3, it is medium if it ranges from 0.5 to 1.9, and low, if the risk level is less than 0.5.

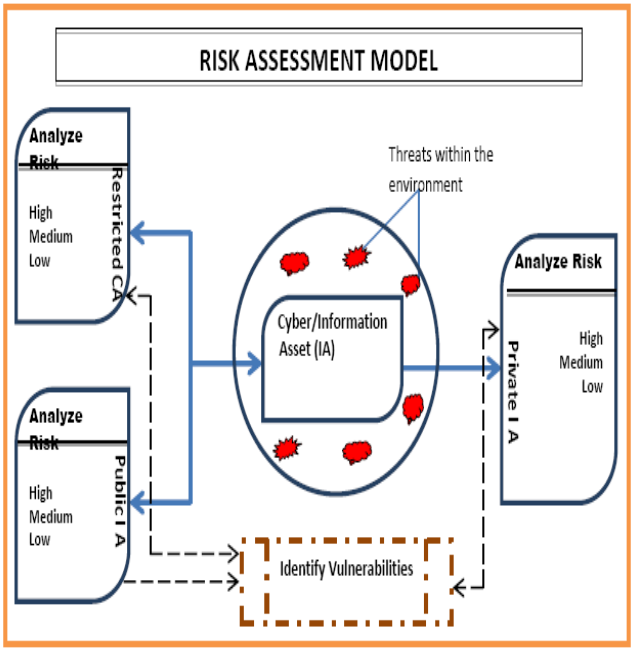

Fig 3: The Cyber-crime control Risk Assessment Model

(B) RISK MITIGATION

Risk Mitigation involves taking actions to eliminate or reduce the probability of compromising the confidentiality, integrity, and availability of valued cyber/information assets to acceptable levels. There are three steps to risk mitigation: identify, choose and implement options.

The options available at the mitigation phase include;

A. Accept the risk
B. Transfer the risk
C. Limit the risk
D. Avoid the risk

- *Accept the Risk*

An organization may choose to simply accept risk under these scenarios of the risk is considered low (e.g., the value of an asset is low and the probability of threats affecting the asset is acceptable) or the cost of accepting the risk is found to be lower than the cost of transferring or limiting the risk. If the cost of accepting the risk is high or more than the cost of transfer or limiting it, then the organization should not accept the risk. The organization should then look at transferring or limiting the risk.

- *Transfer The Risk*

When the risk is transferred, the risk is shared with a third party in part or in whole. This is typically seen in the use of insurance. Third party insurance organizations, for a fee, agree to accept the risk and compensate the information owner for the full damage of a particular risk. In some cases, transferring risk may not be available. In other cases, the risk may be too high and too costly to insure. For example the third party web site hosting. If an organization utilizes a third party vendor to host their website they are transferring some of the risk to the vendor. The vendor is responsible for the availability and integrity of the information supplied by the organization to be posted.

- *Limit The Risk*

When a risk is high for a particular asset, and the risk cannot be transferred (i.e., not practical or cost-effective), then the risk should be limited in part or in full. The process includes identifying the most probable threats to a given asset and identifying, researching, or developing an acceptable control to that threat. In the case of limiting risks such as a virus infection, spam and unauthorized Internet access, the organization may decide to order the purchase of software for all computer devices to reduce the impact of those risks. Risk limiting risk means controlling access to the network, by installing antivirus, spam-ware and a firewall where none exists. Training employees, interns and contractors to be aware of information security also help risk reduction. In some cases, limiting the risk can be fast, inexpensive and sometimes free. Information systems suppliers may provide free security patches and may even provide mechanisms that perform automatic updates to these systems. Applying security updates or bug fixes may simply involve the time and skills of the internal staff.

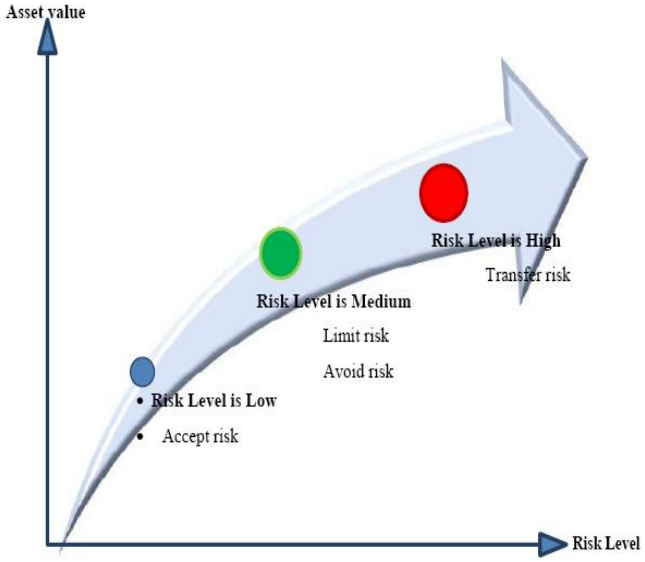

Fig 4: Assets value versus Risk Level

- *Avoid The Risk*

There is no universal answer to when risk avoidance will be appropriate because every circumstance is different. Risk avoidance may be used to protect those assets which are at high risk. Some examples of this option include, create a backup, ping computers systems with confidential information on them disconnected from the Internet.

MATHEMATICAL EXPRESSION OF RISK MITIGATION

Let U, be the corresponding cost value

S be the mitigation mean of the corresponding assets

α be the mitigation cost function

The Mitigation Mean of Assets, S, which is the Average cost value of assets in an organization, can be given as;

ISBN: 978-988-19252-7-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

$$S = \frac{\sum_{i=1}^{n} U_i}{n} \quad (7)$$

Where, U, is the cost value of assets, and n, is the number of assets involved.

Then, the Mitigation Cost Function, α, can be described as high, medium or low as shown in equation (8)

$$\alpha(a_i) = \begin{cases} \text{High}, & S \geq 6{,}000 \\ \text{Medium}, & 5{,}000 \geq S \geq 1{,}000 \\ \text{Low}, & S \leq 9{,}00 \end{cases} \quad (8)$$

This means, the decision on which mitigation option to take, is dependent on the expected mitigation cost.

The Risk Mitigation Decision Function, $F(R)$ is then as formalized in equation (9).

$$F(R) = \begin{cases} accept, & \alpha(ai) = low \ \wedge \ V(ai) = 1 \\ transfer, & \alpha(ai) = high \ \wedge \ V(ai) = 3 \\ limit, & \alpha(ai) = medium \ \wedge \ V(ai) = 2 \\ avoid, & \alpha(ai) = high \ \wedge \ V(ai) = 2 \end{cases} \quad (9)$$

Now, Risk Mitigation involves; *identification of mitigation options, choosing one of the options identified and then implementation of the chosen option.*

Thus, once the organization has identified the various options for mitigating risk, one must be selected. The team or individual designated to handle risk management need to work with the appropriate individuals and make relevant recommendations to management. There is also a need for periodic review of such decisions especially when the information asset changes since the classification of the information asset may change or the threats and risks change.

Implementing the option involves putting into action the choice that has been made for mitigating the risk. As previously defined, the possible actions are to accept the risk, transfer the risk, limit the risk, or avoid the risk. Each information asset now has an assigned risk and the option for mitigating the risk has been chosen. Implementing the chosen option results in certain procedures being followed and/or new controls put in place. Thus, limiting the risk by putting a control in place is the most commonly chosen option to protect the Confidentiality, Integrity and Information systems availability. Observably, continual monitoring and regular update are part of the implementation to keep the risk at a low acceptable level.

IV CONCLUSION

In this paper, the Risk Management procedures of cybercrime control systems were modeled using some mathematical tools. This provides effective deployment of such systems for network security management and threat awareness creation.

REFERENCES

[1] C. Yiseul. (2012), *Strategic Philanthropy for Cyber Security: An extended cost-benefit analysis framework to study cybersecurity*. Working Paper CISL# 2012-06

[2] M. Gercke, (2009), *Understanding Cybercrime. A Guide for Developing Countries*.International Telecommunication Union (Draft).

[3] J.H. Dexter (2002), *The Cyber Security Management System: A Conceptual Mapping*.In Global Information Assurance Certification, SANS Institute, version 1.3.

[4] G. Boughton . (1997), *The Community: Central to Emergency Risk Management.* In Proceedings of the Development Strategies and Partnerships Workshop, Australian Emergency management Institute, Mt Macedon 18-19 November.

[5] O. Akinyokun (2012), *Factor Analytic Approach to cybercrime control.* A Master of Technology Thesis submitted to the Department oc Computer Science, The Federal University of Technology, Akure, Ondo State, Nigeria.

[6] Mark D.(2012), *Cybercrime Survey Report,*The Continuity Center. Accessed at http://www.continuitycentral.com/news06659.html

ISBN: 978-988-19252-7-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)