Volume 5, Issue 1, January 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Risk Management Process Analysis for Data and Communication Devices

[1]Nwagu Kenneth Chikezie, [2]Dr. ObiOkonkwo

[1](M.Sc., PMP, CCNPS, ITIL, MCITP) Doctoral Research Student,
Computer Science Department, Nnamdi Azikiwe University Awka, Nigeria

[2]PhD Student Supervisor & Sub Dean SPGS, Computer Science Department,
Nnamdi Azikiwe University Awka, Nigeria

Abstract— This Research Paper first, defines what data and communication devices are; it's associated types of Security and methods used to "break" security. The risk management process for Data and Communication devices such as Risk assessment, Risk Mitigation and Continuous risk monitoring, evaluation and review. This work also strengthens the fact that the risk is not always negative as reveals by its SWOT (Strength, Weakness, Threat and Opportunity) analysis as one can build on the opportunity thereby reducing the associated threats and also improves on the strengths and invariably reduces and if possible eradicates the weaknesses.

Keywords—Risk, Risk Management, Risk Assessment, Risk Mitigation, Vulnerability, threat, Opportunity

I. INTRODUCTION

Every Organization has vision and mission which is backed with strong Information and Communication Technology (ICT) strategic Planning and Infrastructure. This invariably makes ICT the hub of every promising Organization for better support of her business. In this digital era as Organizations configure automated processes in data and communication devices; Risk Management plays a very critical role in protecting the organizations information assets, and therefore its mission. Risk Management is every stakeholder`s duty and not only for the technical IT team. Hence it should be treated as primarily as an essential role of the Management. An effective and efficient risk management process is an important component of a successful ICT security so as to ensure data confidentiality, integrity and high availability .**Risk** is the net effect of exercise of **vulnerability or opportunity** which can be negative or positive. Vulnerability is the devices` weakness which can be accidentally triggered or intentionally exploited. While opportunity is just positive risk which can be invested upon in order to maximize the use and benefit from the devices. Based on this, Organizations are continuously working on reducing the vulnerabilities by minimizing sources of threats and maximizing the opportunities by strengthening the securities during **SWOT (Strength-weakness-Opportunities and threats)** analysis .**Risk management** is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level, if possible eradicate it completely. The objectives of Risk management in this work are to increase the likelihood and impact of positive events, and decrease the likelihood of negative events in devices. However, before now, Risk management is not consciously or transparently carried out for data and communication devices as the "practice of the day" is that the Organization`s perceived final step in the system development life cycle of the devices is always junking of the devices without final proper risk assessment to ensure that no critical piece of information or data can be intentional or accidentally exploited.

II. WHAT ARE DATA AND COMMUNICATION DEVICES

Data and communication devices are those pieces of equipment or hardware designed to store ,process and transmit information(data and voice) from one point to another .In other words, these allow computers ,desktop phones and other mobile devices to communicate with one another. The communication can take place via a standard network or in workgroup. Among the non-exhaustive list are:

- Router
- Network Interface Card(NIC)
- WiFi Cards
- Modem
- Servers
- Workstations such as Laptops & Desktops
- Phones – both desktop & Mobile phones
- Fax(Facsimile) Machine

- Video Conferencing devices
- Bulletin Board System(BBS)
- Global Positioning System
- Transmission media and all other connectors

Types of Security

Secure communication is when two or more devices are communicating without eavesdropping or interception by a third party. This communication involves sharing of data and information with varying confidentiality and integrity. Among the means to achieve this is:

- Code: This is a means whereby the content and nature of communication is hidden. It is a rule to convert a piece of information and data (for example, a letter ,word, phrase or gesture) into another form of representation, not necessarily of same type.
- Encryption: This is also another means whereby the nature and content of communication is hidden. Here, data and communication is rendered hard to read to any unauthorized party. In some highly security-conscious environments, encryption is configured such that it is a basic requirement for connection and communication to be established. No room for opportunistic encryption which is a lower security method to generally increase percentage of generic traffic and this makes the content susceptible to eavesdropping.
- Steganography: This is sometimes referred to as "hidden writing" in which data can be hidden within another, mostly innocuous data. In this way, it is difficult to find or remove unless you know how to find it.For example in communication, the hiding of important data such as telephone number in apparently innocuous data(an MP3 music file). A good advantage of this is plausible deniability – unless one can prove that the data is there(which is usually not easy),it is deniable that the file contains any.
- Identity based Networks: Unwanted or malicious behaviour is possible on the web since it is inherently anonymous. Identity based network removes the chance of anonymity as the identity of the sender and recipient are known.
- "Security by Obscurity: Similar to needle in a haystack in which secrecy of design or implementation is used to provide security. Though this is discouraged and not recommended by standard bodies. But stakeholders believe that if the flaws are not known, then attackers will be unlikely to find them. As it is known that attacker`s first step is usually information gathering which is delayed by this.
- Random Traffic: This involves creating random data flow to make the presence of genuine communication harder to detect and traffic analysis less reliable.
- Hard to trace routing methods: This method hides the parties involved in a communication through unauthorized third-party systems or relays.

Methods used to "break" security

- Bugging: This is simply known as covert listening device which involves miniature transmitter and microphone. This enables unauthorized parties to listen to conversation.
- Computers (general): Any security obtained from a computer is limited by the many ways it can be compromised – by hacking, keystroke logging, backdoors or even in extreme cases by monitoring the tiny electrical signals given off by keyboard or monitors to reconstruct what is typed or seen.
- Laser audio Surveillance: Sounds including speech inside rooms can be sensed by bouncing a laser beam off a window of the room where a conversation is held and detecting and decoding the vibrations in the glass caused by the sound waves.
- Spoofing: This is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage or access. For example, Caller Id, Email address , IP address etc can all be spoofed.

III. RISK MANAGEMENT PROCESSES

Risk Management involves three main principal processes: risk assessment, risk Mitigation and, Monitor, evaluate and review. All the steps in each process can be broadly summarized as follow:

Risk Assessment:

- Risk identification: This allows individuals to identify risks so that the stakeholders will be in the know of potential threats or opportunities inherent in the devices. It is pertinent to start this stage as early as possible and should be repeated frequently.
- Risk analysis and Priority: Risk analysis transforms the estimates or data about specific risks that developed during risk identification into a consistent form that can be used to make decisions around prioritization. Risk prioritization enables operations to commit resources to manage the most important risks.
- Risk register (Statements): This is the result of risk assessment process. It is a document which contains lists of identified risks, root causes of risks, lists of potential responses, risk owners, symptoms and warning signs, relative

rating or priority list. Risk for additional analysis and responses, and a watch list which is a list of low-priority risk within the risk register.

- Communication and Consultation: There should be steady communication among stakeholders within the organization as everyone is practically involved. In addition to this, the stakeholders can consult the manufacturer of the device through any of the appropriate channels such as through their Representative or customer voices. This ensures speedy and reliable Response.

Risk Mitigation:

- Plan and Schedule risk responses: This step involves process of weighing and developing options and actions to enhance opportunities and reduce threats to the devices.
- Risk mitigation strategies: These are various options through which threats can be reduced and where possible, eradicated (in case of negative risks). However.in case of positive risks - opportunities, they can be enhanced or invested upon. Based on these two sides of a risk, its mitigation options are treated in these lights as well:

Strategies for Negative Risks or threats: There are three main strategies used to deal with threats that may lead to compromise of data/information integrity and confidentiality by exploiting the vulnerability in the devices; If they occur are:

Risk Avoidance: This is used where the risk impact is high. The stakeholders act to eliminate the threats .The most radical avoidance strategy is to shut down the devices or disconnect them from network This may prompt the stakeholders to consult the manufacturers for immediate solution, if there is no other alternatives.

Risk Transfer: Here, the stakeholders shift the impact of the threat to a third party and ownership of the responsibility by use of insurance, warranties, guarantees etc.

Risk Mitigate: In this strategy, stakeholders act early to reduce the probability of occurrence or impact of a risk. Thereby making the risk to be within acceptable threshold

Risk Acceptance: This is used for Negative and Positive risks In this scenario , stakeholders decide to acknowledge the risks and take no action unless the risk occurs. However this strategy provides room for periodic reviews of the threats to ensure that the risk does not change significantly.

Strategies for Positive Risks or Opportunities:

Exploit: This is used for risks with positive impacts on the devices where the stakeholders wish to ensure the opportunity is realised. It seeks to eliminate the uncertainty associated with a particular upside risk by ensuring the opportunity definitely happens. For example, engaging a vast expert to administer the devices who ensures that all the devices` full potential are utilized and also embraces trends of new technologies including their upgrades in order to proactively minimised any vulnerability and negative risks.

Enhance: This is used to increase probability and/or positive impacts of an opportunity. Identifying and Maximizing key drivers of this positive-impact risk may increase the probability of their occurrence. For Example, Changing/upgrading the software (Operating systems, application etc.) and hardware of a device will definitely increase the throughput and security.

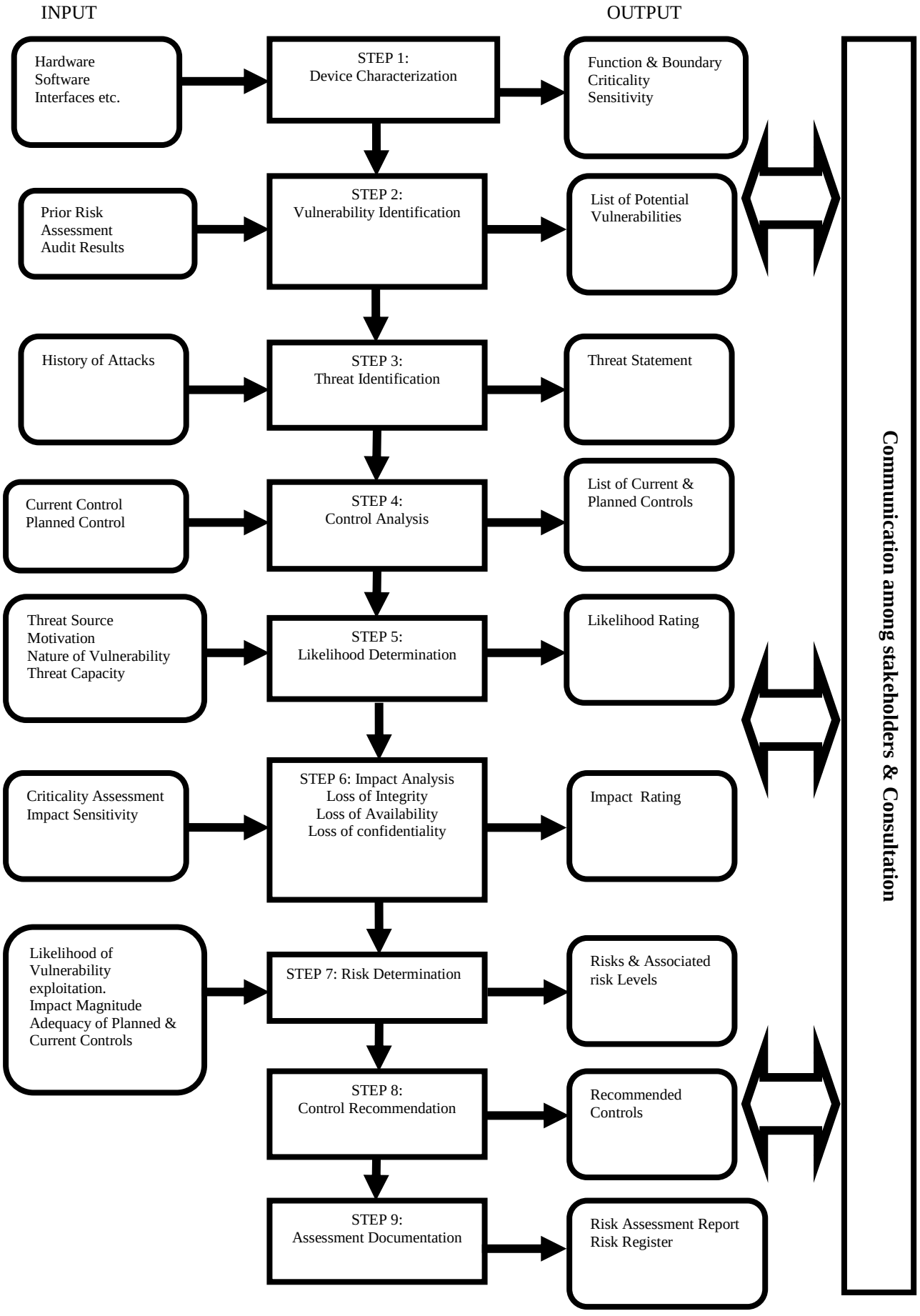
Share: Sharing a positive risk involves allocating some or all of the ownership of the opportunity to a third party who is best able to capture the opportunity for the benefit of the stakeholders. For example, forming a risk-sharing partnership, teams or joint ventures can be established with express purpose of taking advantage of the opportunity so that all stakeholders gain from their actions.

Accept: Accepting an opportunity is being willing to take advantage of the opportunity if it arises but not practically pursuing it

Monitor, Evaluate and Review

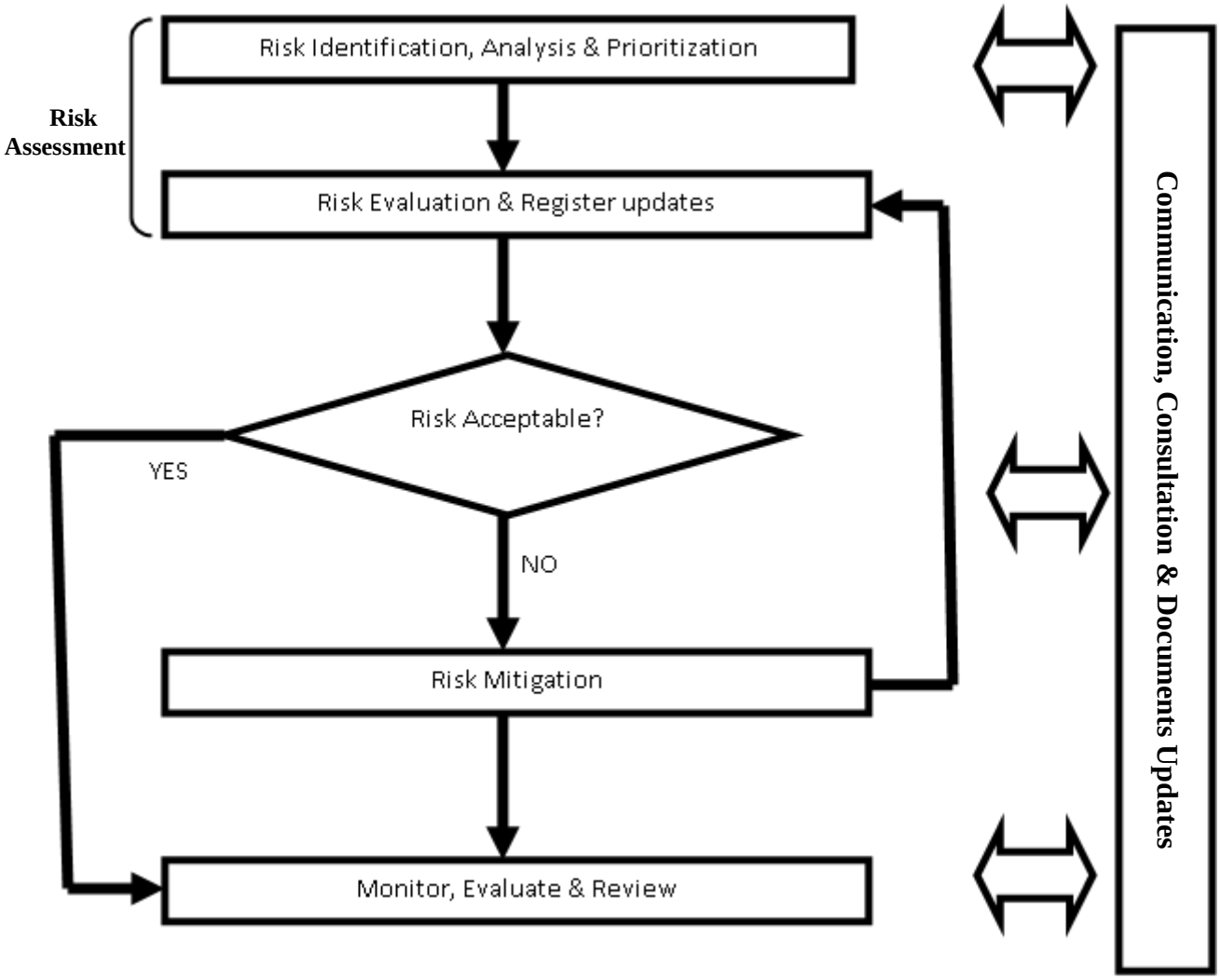
- Monitor, evaluate and Review: Risk management is a continuous process, therefore, all the main stakeholders (technical team especially) must always be checking the devices for new harms and threats considering the present and anticipated vulnerability. As it has been proven that minimizing or eradicating one Risk may trigger another, most times a fresh one or even an undetected one surfaces. This therefore makes monitor, evaluate and review a continuous process throughout life cycle of the devices. The process is very essential in the entire risk management as it links other processes in its course and must be followed with steady communication among the principal stakeholders. Some corporate bodies recommend that this should be biannually. But from my experience as IT Manager – Network and PC, I feel it is better carried out as many times as possible in a year. This is because "eternal vigilance is the price of liberty" according to Wendell Philips
- Lessons learnt and Adapt : This is overall generality of every recommendation,decision,proposed action and of course, action taken with lessons learnt to minimize or completely eradicate a particular negative risks and also to enhance the opportunities of a positive risks associated with the devices. All these, are well-documented for easy retrieval and reference .The document is followed up with consistent updates as new challenges ,discoveries and prospects arise.

Table I: Risk assessment methodology



Adapted from Risk Management guide for information technology systems by Stoneburner G.,Goguen A.,Fering

Table II: Simplify overall risk management process flowchat



IV. CONCLUSIONS

One of the main aims of Risk Management process analysis for data and communication devices is to ensure that the devices are deployed with best of security measures in place, which makes the organization to be fully proactive rather than reactive as it is today with many organizations. This will, invariably increase stakeholders ` risk appetite for positive risks and of course, establish a careful risk threshold for negative risks. This further ensures that cost of attack from a potential intentional attacker is far higher than the anticipated gain. This will likely discourage the attacker. A successful attack has high currency impact, loss of customer confidence and negative business reputation. It assists management to make well-informed risk management decisions to justify the expenditures that are part of an ICT budget and also in authorizing the ICT devices on the basis of the supporting documentation resulting from the performance of risk management.

It is worthy of note here again, that the process is a continuous one in order to get optimal throughput from the devices with little or no down time as a result of attack, vulnerability or negative risks .Thereby increasing the opportunities which the devices can offer. Therefore Risk management continues even at the final stage of systems development Life cycle which is disposal of the devices. It is pertinent to carry out risk assessment at the disposal stage to ensure sensitive data or information are not left out such as vital configurations which may include plain-text passwords ,administrator credentials etc.

ACKNOWLEDGMENT

I would like to express my appreciation to Dr. Obiokonkwo for his mastery guide and supervision; and to Project Management Institute (PMI) USA, for their PMBOK guide fifth edition and other valuable materials on her member Portal.

REFERENCES

[1] Stoneburner G.,Goguen A. and Feringa A.(2001,July). Risk Management Guide for information Systems. Retrieved September 4,2014 from http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.

[2] Radack S.(Ed.).Security for wireless network and Devices. Retrieved August 20,2014 from http://www.itl.nist.gov/lab/bulletns/bltnmar03.htm

[3] Cooney M.(2012,September 21).10 common mobile Security problems to attack. Retrieved August 22,2014 from http://www.pcworld.com/article/2010278/10-common-mobile-security-problems-to-attack.html
[4] A Guide to the Project Management Body of Knowledge(PMBOK) Fifth Edition.
[5] Alshboul A.(2010).Information Systems Security measures and countermeasures: Protecting Organizational Assets from malicious Attacks,3,Article 486878.Retrieved September 10,2014 from http://www.ibimapublishing.com/journals/CIBIMA/2010/486878/486878.pdf
[6] Secure Communication. Retrieved September 9,2014 from http://en.wikipedia.org/wiki/Secure_communication.
[7] http://www.labcompliance.com/tutorial/risk/default.aspx?sm=d_a. Accessed September 9,2014
[8] http://www.iip.kit.edu/english/1680.php Accessed September 7,2014
[9] Risk Management Process Overview. Accessed September 3,2014 from http://technet.microsoft.com/en-us/library/cc535304.aspx
[10] Security through Obscurity. Accessed September 17,2014 from http://en.wikipedia.org/wiki/Security_through_obscurity

