Johnson & Wales University

Providence, Rhode Island

School of Engineering & Design

ISA5010: Research Methods in Information Security

**Comparison of the Effectiveness of Top Security Metrics in Information Technology**

A Research Proposal Submitted in Partial Fulfillment of the

Requirements for the Degree of Master of Information Security/Assurance

**Hardik Adesara**

February 21, 2017

**Table of Contents**

Introduction ……………………………………………………………………………..…… 1

Problem Statement ……………………………………………………………………..…... 2

Background of Study ……………………………………………………………………...... 4

Definition of Terms ………………………………………………………………………..... 10

Research Questions ………………………………………………………………………... 11

Methodology …………………………………………………………………………………. 11

References …………………………………………………………………………………… 16

**List of Tables and Figures**

Figure 1.1: Sequential Exploratory Design **…………………………………………………………………**14

**Introduction**

Every organization for security purposes establishes strategies, plans, management, team work, etc. After this planning step, it is necessary to measure and monitor the effectiveness of that plan. Information technology industry uses security metrics for measuring and monitoring which plays essential role to grow business and keep the system secure. It gives idea about the benchmark- what do organizations want to gain in the future? Also, it helps organizations to decide the baseline of the strategy plans by that means it show where are they in the planning and what is the capacity of teams of doing so?

In organizations, many types of security metrics are used and also need to make sure that information technology industry use the security metrics to secure business. Baseline testing helps to keep business running smoothly and helps to maintain the disaster recovery process.  When performance deviates, set up of programs or products are helpful so that employee can measure all aspects of the performance of the organization. Various types of metrics and comparison of the effectiveness of most used security metrics discussed in other sections of this research proposal.

**Problem Statement**

The organizations related to information technology and information systems that are developed from that technology to successfully carry out their missions and business functions. Threats to information technology industry include environment disruptions, human or machine errors, and purposeful attacks, and so it is significant to prepare for these security disasters, incidents, and threats to face and resolve as soon as possible (NIST, 2010a). It will help to keep the business running safely and securely.

In addition, hackers need only once chance to break an organization’s security plans and system, but as a chief information security officer (CISO) or as a security professional, need to cover and think all possible ways of attack that can shoot on the system (RSA conference, 2010).

Cyber-attacks on information and information systems today are often aggressive, disciplined, well-organized, and well-funded. Attacks can have harmful impacts on organizational operations that include missions, functions, image, and reputation. Security metric is a system of related to measures that enabling quantification of some characteristics and related to dimensions that can be compared against the standards (NIST, 2010a).

According to William Boni the president chief information security officer (CISO) at Motorola Inc., “Security experts cannot measure their success without security metrics, and what cannot be measured cannot be effectively managed.”. It means if vulnerabilities and threats are measurable, and can be expressed in numbers so that it demonstrates the understanding about the organization’s situation.

Each information and information technology related organization or company uses various metrics, depending on the type of business, objective of the business, strategies and size of the organization. First of all, a company needs to decide the clear goal by area, such as risk management, risk assessment, risk mitigation, etc. The next step is to find the broken area of the system and work on how to fix that area. In every information technology industry has one department who provides required technology resources needs to finds the gap in the area of organization. Furthermore, also needs to find out basic functions might not exist in company’s program today and security specialist want to exist in the future and what they are expecting in their department (RSA conference, 2011).

Currently, there is no information about the perfect security metrics for information technology industry. Effective security metrics can play essential role to achieve goals of the organization with limited resources and budgets, so what are the most important criteria to selecting effective security metrics? And what does the technical industry really want from security metrics for growing and secure business?

**Background of Study**

In today’s growing area of information technology, solving security issues is an important task, that is why many approaches and methods are available to response this task (Bakshi, Ahmad, & Kumar, 2011). Information technology industries use security metrics for measuring and monitoring the security performance, establishes new strategies and plans which play a significant role to grow business and keep systems secure.

The main quality criteria of security metrics can help every industry to build security quantification models based on practical needs. In response, there are three necessary quality criteria of security metrics: correctness, measurability, and meaningfulness (Savola, 2013). Security metrics could be an effective factor to achieve security goals for an organization with various components of their security programs like the security of a specific program, product or process, and the ability of staff or departments within an organization to address security issues for which they are responsible (Bakshi, et al., 2011).

In addition, security metrics work on performance scale to achieve baseline to benchmark goal. Every information technology industry needs to prepare for security disasters, incidents, and threats with proper tools and decisions. Security metrics help to ensure the nature and ability of the organization and there is important to know what is happening in the security architecture, and that can be prevent against the security breaches and threats. In result, organization will become a practice and detailed oriented (RSA Conference, 2011). Furthermore, security metrics can be divided into four categories: metrics for measuring the system vulnerabilities, metrics for measuring the defenses, metrics for measuring the threats, and metrics for measuring the situations (Pendleton, Garcia-Lebron, & Xu, 2016). Security metrics have the benefits of gathering data, which helps to improve decision making. It helps to see data in an organized way and without security metrics, data is there in huge amounts but it is invisible.

Metrics are story-driven and help to convert data into a story which gives easy explanation to those at the management level. Sometimes, there is a question of spending money on metrics rather than spending directly on security actions (NIST, 2010b). Basic steps to start with security metrics are: solve complaints from every department, risk assessment and risk management, and find broken things and prioritizing security breaches (RSA Conference, 2011).

To make effective security metrics, there are some primary considerations, as follows:

* **Decision- enabling:** It is wasting time if metrics don’t enable decision makers to do something.
* **Tangible:** Metrics are definable in numbers otherwise who? needs to refine or discard it.
* **Narrative-supporting:** Metrics help to narrate the story in better way and it is not to tell strategy story. If metrics can’t narrate the story, then who? needs to find out why it is there.
* **Data-backed:** Metrics helps to tell story about the organization’s situation and also requires strong foundation which can be explained and demonstrated to anyone at different level. Otherwise, it results into pure theory or fantasy.
* **Repeatable:** Metrics should be easy to gather and update on regular basis; it requires money to gather metrics which is important to remember.
* **Resource-adjusted:** Maintain relationship between your selected metrics and available resources.
* **Discrete:** Metrics need to be broken down to the point which serve the

transparency and data-backing points, it helps to explain.

* **Track what matters:** Do not focus on just trackable, also focus on trackable and

important data and make it easy.

* **Less is usually more:** Performance doesn’t depend on number of metrics, rather it depends on quality and organization (Miessler. 2010).

After considering the above factors, security metrics starts with a specific target area with a clear goal, information security specialist can ensure security metrics results are measurable, actionable, reasonable, and based on a time goal. Various types of security metrics are available in the information technology industry; however, five most used security metrics exist by considering effectiveness (Sun, Chen, Zhou & Min, 2007).

**Patch Latency**

Patch latency explains where an organization stands in terms of the latest updates. An important thing is to understand that applications are people too: that means applications are actual human with human thoughts, and also the combinations of strategy, plans, and experience. Information technology and information systems related organization can include application updates into metrics. Next, if an organization is behind on patching, improve the chances of attackers to easily get into or shoot the system network. The patch management systems are highly powerful to work on the gathered information, and properly convert the data into a symmetrical bell shaped curve which represents how many of them are updated and how many are not. Also, it shows where organization wants that curve to be vs. where it is today (Miessler, 2010).

**Basic Malware Defense Percentage**

Malware defense is appreciated when it has stopped a major Incident. Otherwise, malware defense is just a product which is formally used as an antivirus software. So, basically, it is hard to recognize the strengths of malware defense. The concept of using this metric is to make sure not lose productivity that easily preventable by malware. In addition, an anti-malware system can be considering as a console, it means that can be easily accessible and use. The Basic Malware Defense Percentage metric represents their results by number and percentage, it is demonstrating the current level of performance of organization (Miessler, 2010).

**Password Strength**

This metric is significant in current industry systems. Sometimes it is hard to tell if system is using a weak password or not. Using password strength metric makes it easy to protect systems. These metric deal with proxy for security maturity. sometimes, it requires manual analysis for smaller and custom systems. On the other side, many tools are available to analyze the configured network systems. Most information technology companies preferred that the password strength metric’s results represent by bell shaped curve with five tires (Miessler, 2010; Bonneau, n.d.).

**Change Authorization Percentage**

This metric helps to study the changes in systems by looking at allover percentage of changes took place in the organization. The goal of using this metrics is to identify which changes occur without knowledge of security tracking, Otherwise, it is difficult to detect an attacker. Metric depends on configuration management and a continuous monitoring solution. Again, it is represented by numbers and percentages with detection of separates legitimate changes from unauthorized users (Miessler, 2010; NIST, 2010a).

**Return on Security Investment**

Last but not least, the Return on Security Investment (ROSI) metric helps to keep track of spending money vs. value recovered from the program. The purpose of using the ROSI metric is to know whether a program is worth it or not. ROSI calculation is total spending vs. essential benefits obtained from spending, in terms of risk assessment and saved money. It highly requires for technical industry to find out how much risks are solved, comparing to before and after. Effective ways to represent ROSI’s result by line chart with area map and simple bar chart (Miessler, 2010).

**Conclusion of Security Metrics**

* If the IT industry is to consider quality scale of security metrics with the consideration of above listed effective features, two metrics: Return on Security Investment (ROSI) and Password Strength (PS) metrics give more value to the industries to start with. Return on Security Investment metric gives total benefit of spending and Password Strength can protect systems over hacking. In addition, these metrics follow the less money company have to withhold/spend on insurance, the more money they make.

**Definition of Terms**

Information Security Metrics: Metrics are tools for measuring the effectiveness of security program activities in order to get the most benefits against breaches (NIST, 2010b).

Baseline Performance Scale: the process of understanding of organization’s normal operating environment (NIST, 2010b).

Benchmark Performance Scale: the product testing process used to understand the limits of performance (NIST, 2010b).

MNC: Multinational Corporation or Company

TCS: Tata Consultancy Services

IBM: International Business Machines

**Research Questions**

This study will explore the comparison of the effectiveness of top security metrics. Specially, the study will address the question: “Which security metrics are the most effective out of the top metrics in information technology?”

**Methodology**

To find effectiveness of security metrics in information technology, this study will use a mixed methods research design, because for the information technology industry security metric is an experience, the experience from personal observation, study of past results (in form of numbers and percentage), and the knowledge of information security. This section of the study will discuss the selection of that design and the data collection and analysis.

**Research Design and Rationale**

In this, sequential mixed methods will be used by using information technology industry survey following semi-structured qualitative interviews and quantitative results of security metrics will be used. Quantitative industry results will be analyzed based upon data collected from qualitative phase. Experienced Industry managers will answer security metrics questions, as they will have more knowledge about security and the industry. By using the mixed methods approach, it will make easier to understand and provide quantitative data to confirm the qualitative results. According to Kumar (2011), interviewers have the freedom to decide the format and content of questions related to specific study and the process of asking questions will be very flexible.

**Sample**

Security is a primary concern in the field of information technology, as they have huge amounts of critical data. This study includes the interviews (with security specialist and CISO) and documents (of results of used metrics) with/from three information technology multinational companies: Tata Consultancy Services (TCS), International Business Machines Corporation (IBM), and Infosys**,** because they are most concerned about the security breaches, vulnerability, and disasters. This study will utilize a purposeful sample of industry experience to security metrics. In addition, study gives results in solving security issues by applying individual task and approaching different methods those are already available to response security breaches.

**Instrumentation**

The interviews with three MNC companies will be semi-structured, following interview methods and formal, informative conversation on security metrics. Also, these interviews will be conducted based upon before and after study method (Kumar, 2011). In the initial contact, questions will include “What is current baseline goals of organization?”, “What are the specific criteria will be consider in effective security metrics?”, and “What is future or benchmark goals of organization?” In the second contact, after 3 to 4 months, questions will include “Have you achieved your benchmark goals with specific security metric(s)?” The analysis of the interview and contacts will result in creation of the instrument for the survey.

**Data Collection**

Data collection procedure will occur in the interview phase by knowing organization’s personal experience, observations, results of used security metrics, and obtaining information regarding the effectiveness of the security metrics used to meet the goals of the organization. This will be beneficial to the managers and CISO, as the interviewer will have more information after taking surveys from different organizations and interviewer will be giving feedback to the company.

In addition, focus groups will be used to get better idea of the security metrics. Groups of information security specialists will include PhD professors and industry experienced professionals, where advantages and disadvantages of top security metrics will be discussed.

**Data Analysis**

Data analysis will include examination of notes taken during interviews, documentation of the companies, recorded interviews and data collected from the survey instruments. Each of these will provide data that will be analyzed using a sequential exploratory design:

**Figure 1.1. Sequential Exploratory Design**

quantitative

QUALITATIVE

Next, baseline and benchmark goals will be compared based upon company’s experience and results after using security metrics and seeing the goals and results achieved by them. Focus group data will be analyzed by reviewing notes, experience and recovered videos (Kumar, 2011).

**Limitations**

The study has limits in the areas of authentication and security. Security metrics experts are not often open to discuss their goals and problems they faced in the past. Also, specialists will not be agreed upon some instruments to provide authenticate answers and data because of security, rules and regulation purpose of the organization.

Some specialist provides information based upon their knowledge and research not based upon experience which can distract from real data.

**Delimitations**

The study will be limited to three multinational companies (MNC) of information technology, and those are Tata Consultancy Services (TCS), International Business Machines Corporation (IBM), and Infosys. Other nontechnical industries will be excluded because security metrics are essential and important for the information technology world.

**Resulting Actions**

This study will seek to determine the most effective security metrics for the information technology industry on how to achieve their benchmark goals in the area of improvement, performance, competition, and security. In addition, this study will be of a benefit to multinational companies in the information technology field for measuring and monitoring the security performance of their organization. Also, it will help identify new strategies and plans which play a significant role to grow business and keeps systems secure.

**References**

Bakshi, A., Ahmad, K., & Kumar, N. (2011, July). Security metrics: Needs and myths. *International Journal of Operations Research and Optimization*, *2*(2), 303-314.

Bernik, I., & Prislan, K. (2016, September). Measuring information security performance with 10 by 10 model for holistic state evaluation*.* *PLOS One* *11*(9).

Bonneau, J. (n.d.). Statistical metrics for individual password strength. *University of Cambridge*. Retrieved from http://www.jbonneau.com/doc/B12-SPW-statistical\_password\_strength\_metrics.pdf

Goldfarb, J. (2015, June 9). Security metrics: It’s all relative.  Retrieved from <http://www.darkreading.com/analytics/security-metrics-its-all-relative/a/d-id/1320772>

Kumar, R. (2011). *Research methodology: A step-by-step guide for beginner*. London, UK: SAGE Publications.

Miessler, D. (2010, April 5). An information security metrics primer*.* Retrieved from <https://danielmiessler.com/study/information-security-metrics/#gs.FpxFgng>

National Institute of Standards and Technology (NIST). (2010, February). Guide for applying the risk management framework to federal information systems: A security life cycle approach*.* Retrieved from <http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf>

National Institute of Standards and Technology (NIST). (2010, June). Guide for assessing the security controls in federal information systems and organizations: Building effective security assessment plans*.* Retrieved from http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf

Pendleton, M., Garcia-Lebron, R., & Xu, S. (2016, January). A survey on security metrics. *Cornell University Library*. Retrieved from https://arxiv.org/abs/1601.05792

[RSA Conference]. (2011, July 12). RSA conference 2011 - Security metrics: A beginner's guide - Caroline Wong. [Video File]. Retrieved from https://www.youtube.com/watch?v=dFsbqGJ3qEY

Santander Peláez, M. H. (2010, April 5). Measuring effectiveness in information security controls. *SANS Institute InfoSec Reading Room*. Retrieved from <https://www.sans.org/reading-room/whitepapers/basics/measuring-effectiveness-information-security-controls-33398>

Savola, R. M. (2013, September). Quality of security metrics and measurements. *Computers & Security 37*, 78-90.

Singleton, J. P., McLean, E. R., & Altman, E. N. (1988, June). Measuring information systems performance: Experience with the management by result systems at Security Pacific Bank*.* *MIS Quarterly,* *12*(2), 325-337.

Sun, G., Chen, Y., Zhou, Z., & Min, Z. (2007, November). A configurable access control system for networked manufacturing monitoring using XML. *International Journal of Advanced Manufacturing Technology, 39*(11), 1252-1261.

Wu, M.-Y., & Yu, M.-H. (2013, October 15). Enterprise information security management based on context- aware RBAC and communication monitoring technology. *Mathematical Problems in Engineering, 2013*, 1-11.