I. Information Security Maturity Model

Dr. Malik F. Saleh
msaleh@pmu.edu.sa
Management Information Systems, Chair
Prince Mohammad Bin Fahd University
Al Khobar, 31952, Saudi Arabia

Abstract

To ensure security, it is important to build-in security in both the planning and the design phases and adapt a security architecture which makes sure that regular and security related tasks, are deployed correctly. Security requirements must be linked to the business goals. We identified four domains that affect security at an organization namely, organization governance, organizational culture, the architecture of the systems, and service management. In order to identify and explore the strength and weaknesses of particular organization's security, a wide range model has been developed. This model is proposed as an information security maturity model (ISMM) and it is intended as a tool to evaluate the ability of organizations to meet the objectives of security.

Keywords: Maturity Model, Security Maturity Model, Security Measure, Security self study.

1. INTRODUCTION

The traditional information security objectives are confidentiality, integrity, and availability. Achieving these three objectives does not mean achieving security. Security is achieved by the prevention of attacks against information systems and from achieving the organization's mission despite attacks and accidents. One problem with organizations' security is that it is often viewed in isolation and organizations do not link the security requirements to the business goals. The rationale for these organizational problems is linked to the financial obligations that organizations face for unnecessary expenditure on security and control. Some of the information security efforts may not achieve the intended business benefit, resulting in lack of security and financial investments in systems that do not represent the core systems of an organization. For example managers can justify the need for a system that manages the resources at an organization. It is a relatively simple task to identify a system that adds value to an organization but to justify a second system to protect the first one might result in cancelling the investment of both systems. Any additional security investments are thought of as future projects that can wait until the business prospective is improved. Then, organizations are faced with the challenging task of recovering from an attack that disrupts the business process.

To ensure security, it is important to build-in security in both the planning and the design phases and adapt a security architecture which makes sure that regular and security related tasks, are deployed correctly [1]. Security requirements must be linked to the business goals through a process-oriented approach. The process must take into consideration many of the factors that affect the goals of an organization. We identified four domains that affect security at an organization. First, organization governance is one factor that affects the security of an organization. Second, the organizational culture affects the implementation of security changes in the organization. Third, the architecture of the systems may represent challenges to the implementation of security requirements. Finally, service management is viewed as a challenging process in the implementation.

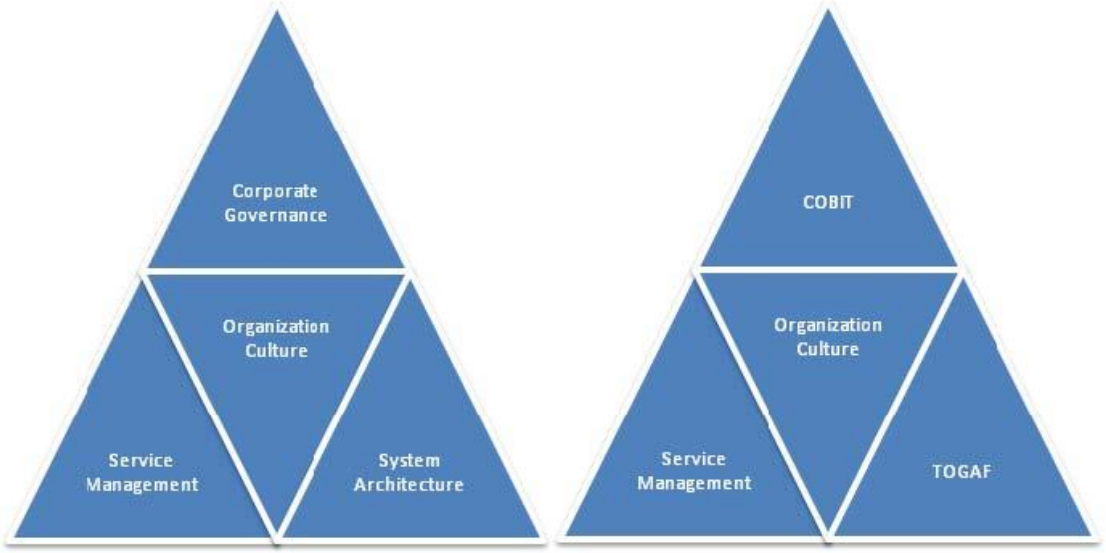

Figure 1: Domains mapped to implementation standards

This research narrows the gap between theory and practice for information security management by following the process of a security maturity model and by identifying the benefits of implementing a standard for organization security needs. We stress the fact of using a domain based approach to develop a model that can be widely used by organizations. This approach, if developed without an understanding of the organizational culture, will impact the effectiveness of the implementation and the human reaction to the use of new technologies. The organization culture often hinders the success of this approach and the delivery of the intended benefits of the implemented security model or standard.

1. BACKGROUND AND RELATED WORK

The motivation for this paper was due to challenges of assessing the implementation of security at organizations. In addition to implementation challenges, accomplishing best practices in the implementation of security is needed and it was undertaking in this research in the form of a self study that organizations would use to measure their information security practices.

Some attempt were undertaken to establish information security management maturity model. The ISM3 system was introduced to prevent and mitigate attacks, errors, and accidents that jeopardize security [2]. While this attempt recognized three levels of management responsibility, it did not provide best practices for the implementation of security.

An information assurance model was introduced based on none risk assessment model. It is based on diligence model where assurance is achieved by using threat and vulnerability reviews and countermeasures based on tangible best practices. The model did benchmarking, risk assessment and followed a diligence model [3]. This model introduces benchmarking but it did not provide best practices for security.

A certification and accreditation model through the identification of operational risks and the determination of conformance with established security standards and best practices was introduced by [4]. Its idea was to effectively establish trustworthiness for security services. While an organization policy and defined processes will introduced by [5] with appropriate accountability standards to facilitate compliance, monitoring and enforcement of security guidelines.

2.1 Domain-Oriented Approach

Senior management at organizations must become more IT literate to effectively synergize business strategy. In security, people, information, systems, and networks affect each others. These four domains provide a vital link to all of the dynamic interconnections at an organization. Inside each domain, there are processes that identify, measure, manage and control risk.

Connecting different domains together requires securing each domain and securing the interconnection between the different parts. For the purposes of creating a widely used model that has good practices, security is looked at as domains, were each particular category of security represents knowledge in the organization. According to [6] there is no one-size-fits-all approach for maximizing the alignment of IT with the business and all of its components. Much depends upon the nature of the business, its size, markets, culture, and leadership style. Additional factors that help dictate the organization's alignment components and structure include the in-house IT capabilities and the dependence upon outsourcing.

2.1 Maturity Model

The concept of maturity models is increasingly being applied within the field of Information Systems as an approach for organizational development or as means of organizational assessment [7-9]. Any systematic framework for carrying out benchmarking and performance improvement can be considered as a model and if it has continuous improvement processes it can be considered a maturity model. Maturity implies a complete system. Generally, in the constituent literature maturity implies perfect or explicitly defined, managed, measured, and controlled system [10]. It is also a progress in the demonstration of a specific ability or in the accomplishment of a target from an initial to a desired end stage.

The Total Quality Management (TQM) maturity models is a structured system for meeting and exceeding customer needs and expectations by creating organization-wide participation in the planning and implementation of breakthrough and continuous improvement processes. It integrates with the business plan of the organization and can positively influence customer satisfaction and market share growth [11]. This structured system encompasses the entire organization and the goal is communicated on a regular bases while practicing what is being breached [12]. Quality can take many forms but its perception is dependant on the beholder. However, the emphasis is on things being done right the first time.

In order to identify and explore the strength and weaknesses of particular organization's security, a wide range model has been developed. The purpose is to identify a gap between the practice and theory which then can be closed by following a process-oriented approach. We introduce a maturity model that provides a starting point for security implementation, a common and shared vision of security, and a framework for prioritizing actions. Moreover, this information security model has five compliance levels and four core indicators to benchmark the implementation of security in organizations.

1. INFORMATION SECURITY MATURITY MODEL (ISMM)

This proposed information security maturity model (ISMM) is intended as a tool to evaluate the ability of organizations to meet the objectives of security, namely, confidentiality, integrity, and availability while preventing attacks and achieving the organization's mission despite attacks and accidents. The proposed model defines a process that manages, measures, and controls all aspect of security. It relies on four core indicators for benchmarking and as an aid to understanding the security needs in the organization. These indicators are goal-driven to achieve the security needs.

3.1 Levels of Compliance

It is hard for security practitioners and decision makers to know what level of protection they are getting from their investments in security. It is even harder to estimate how well these investments can be expected to protect their organizations in the future as security policies, regulations and the threat environment are constantly

changing [13]. An information system would transition between several distinct vulnerability states. The first state is hardened and it occurs when all security-related corrections, usually patches, have been installed. The second is vulnerable and it occurs when at least one security-related correction has not been installed. The final state is compromised and it occurs when it has been successfully exploited [14]. Within these states, metrics need to indicate how secure the organization is so that the window of exposure can be minimized by the security operations teams in an organization by following a standard patching process to eliminate vulnerability and any associated risks. The security team either deploys patches after vulnerability was first disclosed or updates signatures that are associated with attacks.

The longer the window of exposure, the more the organization is exposed to attacks and exploits. The magnitude of risks is minimized if organizations are conscious about their security needs. Therefore the proposed ISMM considers five levels of compliance. Security is believed to improve as the organization moves up these five levels:

Figure 2: Levels of Compliance

3.2 None Compliance

This state is characterized by none existence of policies and procedures to secure the business. Management does not consider investing in security related systems necessary for the overall business strategies. In addition, the organization does not assess the business impact of its vulnerabilities and it does not understand the risks involved due to these vulnerabilities.

3.3 Initial Compliance

This state is the starting point for any organization. As long as an organization is conscious about the threats that their information systems face then that organization is considered in the initial state of compliance. This state is characterized by being chaotic, inconsistent, ad hoc, and in response to attacks and possibly because of losing resources due to an attack. Organizations recognize the business risks due to vulnerabilities but have no defined policies or procedures to protect the organization. In addition, the organization would have little practical implementation in security systems. Most implemented control will be reactive and not planned.

The goals at the initial state are usually centered on the business activities of the organization and little attention is focused on securing the organization. The goals will change in response to attacks by implementing some kind of protection but it will not be continuous.

3.4 Basic Compliance

This state is the starting point for any organization that wants to protect its investment and ensure continuity. Application and network security is implemented but changes are not centrally managed and ad hoc security requests are common. In this state, organizations trust the interaction between the user and the systems. Security awareness programs are being considered for key resources only. IT security procedures are informally defined and some risk assessments taking place. In addition, responsibilities for IT security have been assigned but enforcement is inconsistent. Some intrusion and detection testing can also be performed.

A fundamental process to most systems is the interaction between the system and the user. According to [15], this interaction is the greatest risk. Organizations don't classify their users as threats to their systems. The user does not always cause a threat in isolation; rather, the actions of users are the starting point for some attacks, and in some cases, the users themselves may launch the attacks. Weak passwords, susceptibility to social engineering attacks, and failure to install security updates are some examples of why the user is classified as the weak human factor and the user's interaction with the systems create threats [16].

The goals at this level are usually centered on the business activities of the organization and the protection of core systems. Usually, an organization will consider the security of a system after the system's implementation. Two restrictions are faced at this stage: First, financial restriction and spending on systems that don't add value to the income of the business. Second, organizations classify their initial investments in security as completed. Organization will have a perception that their systems are protected and they become unaware of the threats and vulnerabilities.

3.5 Acceptable Compliance

This state is characterized by central management of all security related issues and policies. Users are trusted but their interactions with the systems are viewed as vulnerability. No ad hoc changes and central configuration models, from which all configurations are derived, are implemented. Security policies and procedures are now in place together with adequate delivery mechanisms to aid awareness and compliance. Access controls are mandatory and are closely monitored. Security measures are introduced on a cost/benefit basis and ownership concept is in place.

There is a school of thought that maintains that it is not the users' fault that they perform the easiest action; rather, it is the designers fault to have made the most insecure operation the easiest operation [16]. Since the actions of users are the starting point for some attacks, there is a need to inculcate a "culture of security" in users. Many users have to remember multiple passwords. They use different passwords for different applications and have frequent password changes, which reduces the users' ability to remember passwords and increases insecure work practices, such as writing passwords down [17]. For organizations to secure the interactions with their systems, communication between the security team and the users must take place to keep the users informed of possible threats. In addition, the users do not understand security issues, while the security team lacks an understanding of users' perceptions, tasks, and needs. The result according to [16] is that the security team typecast the users as threats that need to be controlled and managed, at worst, they are the enemy within. Users, on the other hand, perceive many security mechanisms as an overhead that gets in the way of their real work.

The goals at this state are usually centered on the business activities, the users, and monitoring security threats and all related patches are tested and implemented. Usually, organizations at this state are conscious about their security needs and they invest in systems that protect the organization.

3.6 Full Compliance

This state is characterized by having control over the security needs of the organization, monitoring the systems, being aware of threats and benchmarking by comparing the organization itself to other similar organizations and to international standards. In addition, a comprehensive security function has been established that is both cost effective and efficient which delivers high quality implementation. This comprehensive plan has formal policies

and procedures in place to prevent, detect, and correct any security related issues. Also, corporate governance is aligned with the security needs of an organization. Corporate governance has policies for internal auditing which is independent and objective activity designed to add value and improve the security of the organization. The result of any audit activity is published and actions are implemented.

For organization to have full compliance security is managed by identifying the security concerns and security incidents are tracked in a systematic way. The organization must have proper policies for security in a formal sense and business plans would have items for security. The use of specific technologies throughout the organization is in a uniform manner and the implementation came to existence out of a business plan.

Full compliance also considers the security architecture in an organization. While the business architecture considers all external factors in an organization, the security architecture considers all users in the implementation. Policies are created to meet the needs of the users but information in or out of the organization is captured. A system for providing traceability through the organization is in place. Users are also involved in architectural analysis and the organization offers training for the users in security related issues.

As for management of security, policies in the full compliance state have preventive, detective and corrective control. The organization must have a system for reporting security incidents and for tracking the status of each incident. Installing anti-virus software and firewall is not enough to control the threats the organizations face. Email filters and intrusion detection systems must also be used to prevent many types of incidents.

1. MEASUREMENTS

Metrics are often used to predict future behaviors, based on historical data and trends.[13] argue that Security metrics are created and monitored as a way to get insights about the performance of these controls and to identify failure points or anomalies. However, the metrics are collected across organizations and they are operational metrics without the context of the overall security processes. On the other hand, measurement of any complex, operational system is challenging and security risks introduce another dimension of complexity. Risk management and the availability of different measurements and their properties will vary during the overall system lifecycle. Any measurement framework needs to be able to adapt to both the changes in the target of measurement and in the available measurement infrastructure. Security assurance measurements often require aggregation of several metrics, because direct measurement of the relevant properties is not often possible in practical complex systems and aggregation strategies can change from time to time, depending on the environment and the many risk factors [18].

4.1 ISMM Metric and Core Indicator

The principle that is followed here is what you can't measure, you can't manage. Therefore four core indicators are developed to manage and measure the compliance with this maturity model. Each indicator has its own key performance indicators that show the overall compliance with the model. These four indicators are domain specific rather than being process specific but they measure the aspect of structure, the management, the practices and the overall performance of the of the organization in term of its security.

The specific practices are intended as a guide for those responsible for the activities to draw their attention to good practices and to assist them to evaluate the practices at their organization. For each individual item, two responses are called for, but some items may not be applicable to the organization, therefore it should be marked with NA and ignored. The second response if applicable should be measured in term of assigning a five points rating scale to evaluate how well the practices are carried out. Certain activities require combining ratings to develop a broader rating. An overall rating of all domains would reflect the compliance with this maturity model according to table 1.

1. LIMITAION, IMPLICATION, AND RECOMMENDATION

The results of this paper clearly showed that there are metrics that can assess the implementation of security at organization. However, the use of a qualitative method incorporates various disadvantages and it is often criticized for being subjective and it lacks criteria to judge the trustworthiness and relevance of the results.

Much more research needs to be undertaken to accomplish best practices in the implementation of security by using a combination qualitative and quantitative research. Quantitative work will be undertaken to demonstrate the effectiveness of the proposed model. A survey of will be distributed to different organization and the result will be published in the near future.

1. CONCLUSION AND CONTRIBUTION

A systematic framework for carrying out benchmarking and performance improvement was developed. This model of best practices can be considered a maturity model which implies a complete system with continuous improvement. The objective of the proposed solution is to provide an organization with a way to conduct a self study of its implementation of security. The result will be measured in terms of compliance to the model. There are five compliance levels and each level consists of goals. An organization that continuously measure and audit its security implementation will achieve the highest level and it will achieve the objectives of security.

Full compliance to the model is characterized by having control over the security needs of the organization, monitoring the systems, being aware of threats and benchmarking by comparing the organization itself to other similar organizations and to international standards. Acceptable compliance is characterized by central management of all security related issues and policies. Other levels exist to raise a red flag for organizations that their security is weak and improvements are required.

The measurement indicators were domain specific rather than being process specific but they measure the aspect of the structure, the management, the practices and the overall performance of the of the organization in term of its security.

1. **REFERENCES**

1. Amer, S.H. and J. John A. Hamilton, *Understanding security architecture*, in *Proceedings of the 2008 Spring simulation multiconference*. 2008, Society for Computer Simulation International: Ottawa, Canada. p. 335-342.
2. Aceituno, V. *Information Security Management Maturity Model* 2007 [cited 2011 July 11]; Available from: www.ism3.com/page1.php.
3. Al-Hamdani, W.A., *Non risk assessment information security assurance model*, in *2009 Information Security Curriculum Development Conference*. 2009, ACM: Kennesaw, Georgia. p. 84-90.
4. Lee, S.W., R.A. Gandhi, and G.-J. Ahn, *Establishing trustworthiness in services of the critical infrastructure through certification and accreditation.* SIGSOFT Softw. Eng. Notes, 2005. **30**(4): p. 1-7.
5. Walton, J.P., *Developing an enterprise information security policy*, in *Proceedings of the 30th annual ACM SIGUCCS conference on User services*. 2002, ACM: Providence, Rhode Island, USA. p. 153-156.
6. Williams, P.A. *IT Alignment: Who Is in Charge*. [cited 2011 May 21]; Available from: http://www.isaca.org/Knowledge-Center/Research/Documents/IT-Alignment-Who-Is-in-Charge.pdf.
7. Ahern, D., A. Clouse, and R. Turner, *CMMI distilled: A practical introduction to integrated process improvement*. 2004, Boston, London: Addison-Wesley.
8. Chrissis, M.B., M. Konrad, and S. Shrum, *CMMI: Guidelines for Process Integration and Product Improvement*. 2008, Upper Saddle River, NJ: Addison-Wesley.
9. Mettler, T. and P. Rohner. *Situational Maturity Models as Instrumental Artifacts for Organizational Design*. in *Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology*. 2009. Philadelphia, Pennsylvania: ACM.
10. Fraser, M.D. and V.K. Vaishnavi, *A formal specifications maturity model.* Commun. ACM, 1997. **40**(12): p. 95-103.
11. V., P.P. *Total Quality Management - A Strategic Initiative Gaining Global Compitative Advantage*. 2010 May 21 [cited 2011; Available from: http://www.indianmba.com/Faculty_Column/FC1174/fc1174.html.
12. *TQM - Total Quality Management*. 2003 [cited 2011 May 21]; Available from: http://www.six-sigma-material.com/TQM.html.
13. Beres, Y., et al., *Using security metrics coupled with predictive modeling and simulation to assess security processes*, in *Proceedings of the 2009 3rd International Symposium on Empirical Software Engineering and Measurement*. 2009, IEEE Computer Society [download]. p. 564-573.

14. Arbaugh, W.A., W.L. Fithen, and J. McHugh, *Windows of Vulnerability: A Case Study Analysis.* IEEE Computer, 2000. **33**(12): p. 52 - 59
15. Schneier, B., *Secrets and Lies: Digital Security in a Networked World*. 2000, New York: John Wiley & Sons, Inc.
16. Vidyaraman, S., M. Chandrasekaran, and S. Upadhyaya, *Position: the user is the enemy*, in *Proceedings of the 2007 Workshop on New Security Paradigms*. 2008, ACM: New Hampshire. p. 75-80.
17. Brostoff, S. and M.A. Sasse, *Safe and sound: a safety-critical approach to security*, in *Proceedings of the 2001 workshop on New security paradigms*. 2001, ACM: Cloudcroft, New Mexico. p. 41-50.
18. Kanstrén, T., et al., *Towards an abstraction layer for security assurance measurements: (invited paper)*, in *Proceedings of the Fourth European Conference on Software Architecture: Companion Volume*. 2010, ACM: Copenhagen, Denmark. p. 189-196.