SECURING INFORMATION ASSETS: A FRAMEWORK FOR THREAT MODELING AT THE ORGANIZATIONAL LEVEL

Elsaleiby, Aber [(a)] and Kunnathur, Anand [(b)], University of Toledo, College of Business and Innovation, 2801 W. Bancroft St., Toledo, OH, 43606
(a) Aber.Elsaleiby@rockets.utoledo.edu, (b) Anand.Kunnathur@utoledo.edu

ABSTRACT

Threat Modeling as a mechanism, in Information Security, has been deployed in organizations primarily to get a handle on the nature, scope, severity and potentiality of technical level threats to information assets. In this paper, we address the issue of developing and understanding of threats to information assets at the organization and inter organizational levels, with a view to further develop proactive management models and guidelines for anticipating and mitigating the consequences of such threats. To this end, we survey relevant literature and provide a framework for addressing the modeling of threats at the organization and inter organizational levels.

INTRODUCTION

Information is an integral part of all organizations. Dhillon (2007) defined organization as a series of information handling activities that become more complex as organizations grow. Further, information is a critical asset that is essential for not only operating the production and service activities of organizations, but also to develop realistic strategic plans and, in particular, to shape inter-organizational collaborations (Veen-dirks and Verdaasdonk, 2009). The rapid advances in information technology and communication make information access prevalent and consequently a highly vulnerable asset that must be secured.

"Threat modeling" is a method of evaluating and documenting the security threats (Swederski and Snyder, 2004). Building such a model is based on the first place on identifying sources of threats and how they can be managerially controlled. Securing information related to employees, vendors, customers, financial transactions against all possible threats, while continuing to provide for and benefit from data and idea sharing through relatively easy information access becomes a pressing need for organizations. While there have been attempts at modeling the threats associated with information at the software (and compact systems) level, there are no comprehensive mechanisms in place to do threat modeling to anticipate and mitigate risk of security compromises at the organizational information management level (Hagen et al., 2008). Perhaps, this is partly due to the decentralization of the information management activities in organizations over the past two decades. This decentralization itself is a contributor to the elevation of the information security risk, because of the lack of awareness and absence of cohesive policy on how to handle information flows and management of the information resource, especially, across functional area boundaries (Vacca, 2010). We propose to address this issue through the development of the research framework for threat modeling for the information resources of the organization as a whole, leading to better and sustainable threat modeling of local information systems and resources.

Within the context of information security, aspects of management have been generally defined in ISO 27001, Information Security Management Systems Standard, as "that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve Information Security." Achieving this business risk management approach requires a careful consideration of "organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources."

Dhillon (2007) identified the different managerial aspects of information security through "the fried egg analogy" in which he depicted three aspects of managing information security: technical, formal, and informal. Since security is all about maintaining the integrity of the three levels, linking the threats to information management at each of the three levels will be helpful for managers to set their goals, policies and procedures needed to control for security of the data. Although there is a huge body of literature that identified threats besides those literatures that covered the management aspects of information security, none of the literature linked the two nor showed what can really be managerially controlled.

The aim of this research is to develop an information security threat modeling framework that ties together the technical and non-technical aspects of the security threat. The framework will identify the different types of threats a manager may face, and it will also indicate how they can be controlled. The framework would have the potential to work as a mechanism for the development of a measure of: (1) the level of threat that would exist within the firm; (2) the controllability of threat. It will work as a management tool that enables prioritizing threats, from the organization's perspective, and accordingly commit and deploy, in timely fashion, resources needed to mitigate the risk. Thus, such a framework for Threat Modeling of the Information Assets of the Organization (TMIO) can be used as a proactive management tool to anticipate and mitigate the security risks, without having to scramble, frequently, to react to security breaches. In so doing, the organization can enjoy fewer disruptions of its operations, while expending far fewer resources than would be needed to do damage control, in purely reactive mode (Farn et al., 2004). This will help the organization to prioritize threats based on the likely harm that could result from the realization of the threat, the budget available and the controllability. The current research is based on the fried egg model (Dhillon, 2007) and its extension (Menon and Kunnathur, forthcoming) that identify the levels that impact information security in the organization and between organizations and the scope of managerial control. We hypothesize that managers can fully control threats at the technical, and the formal level; however, they can only partially control the threats at the informal level.

The first step we have taken toward developing such a modeling framework is to meticulously identify the different types of information threats the business may be subjected to. Then, we will show the proposed security model in order to enable organizations to develop mechanisms and policies to manage the various threats, mitigating the associated risk to the organization.

LITERATURE REVIEW

Development of the area of information security over time was a point of concern of Solms (2000) who classified the development of information security into three main waves: technical wave, management wave that is characterized by realization and involvement of information security, and the third wave is institutional wave that is characterized by the best practices and code of practices of information security.

Literature within the context of information threat can be classified into two categories; one that intensively focuses on the technical aspects of threats (Gordon et al., 2006; Carey, 2008), while the other focuses on the "non-technical aspects" of threats which deals with human and organizational challenges to information security. Despite the criticality of both and the acknowledgement of the perception of threat and security as well as the culture of information security within organization, less attention was directed toward human and organizational aspects as major challenges to today's information security (Anderson, 2007).

The managerial aspect of information security was intensively studied by different researchers like Ashenden (2008) who clearly indicated that organization wide protection of information, in all its forms, requires us to go far beyond just providing security through only technical means. Rather, it entails moving toward a business wide means which, in turn, necessitate an integrated view point that should not only be limited to providing confidentiality, integrity and availability of information but also to include both protecting and facilitating information sharing as well as managing the associated risks resulting from the ever increasing number of threats that are continually changing. The author argued two different approaches to secure information, managed and unmanaged approaches. The unmanaged approach to information security is likely to cause a chaotic implementation of the different ways of security controls that results from the high chance of inadequately identifying the different threats and risks linked to them which, in turn, lead to inappropriate or overelaborated controls. The author stated that "without management it will be difficult to understand what has been done, why, by whom and for what purpose." Conversely, managed information security will ensure the, 'selection of adequate and proportionate security controls that protect information assets and give confidence to third parties' (ISO 27001).

Examples of the different types of threats covered in the literature will be discussed in this review as follows:

Threat Types

Before presenting the threat types widely covered in the literature, we need to first define what information system threat is. Threat to information system is a condition in which harm, loss or damage to information could occur through one of four ways identified by Wilson et al. (1992): (1) destruction: the asset is not reparable or recoverable, (2) modification: altering an asset by changing its representation or adding more to the representation, (3) disclosure: information is accessed by or released to someone lacking a need-to-know; and (4) denial of services: resources are unavailable to authorized users. Other researchers, such as (Dhillon, 2001) have extended this taxonomy where threats can be classified based on the asset involved. For example, (Icove et al.,

1999) found that threats can occur on seven different areas: software, hardware, data, network, physical, personnel, and administration (including security regulations and policies). In addition, Whitman and Mattord (2008) differentiated between attacks and threats and they identified twelve major threats and fifteen types of attacks. Haung et al. (2010) identified "the most common 21 information security threats" that they further grouped under the twelve major threats previously addressed by Whitman and Mattord (2008).

From the managerial perspective, threats can be broadly classified into: (1) threats that arise due to lack of technical control that are mainly related to hardware, software, network and people; (2) threats due to lack of formal managerial control in the form of procedures, regulations, governance, rules and policies; and (3) threats due to problems within the social and communication pattern of organization (informal type of threats). A closer look into each threat class enables us to make the following inferences: the first threat class focuses on the technical related threats like malicious ware, hardware, software, and network failure,….etc. On the other hand, the second class stresses the threats related to lack or absence of governance, disobedience of policies, procedures and guidelines. Among these threats are conflicting rules, lack of accountability, and over bureaucratization. The third and last class obviously focuses on people and the social communications. Here, it should be pointed out that both formal and informal threat related aspects are complex to control.

THREATS RELATED TO TECHNICAL ASPECTS

Threats that occur at the technical level can be viewed from four broad scopes: software, hardware, networking, and data. This class of threats can be due to one of these possible causes: modification, destruction, unintentional loss, theft, interception, interruption, disclosure and fabrication, however, disclosure and fabrication are only data related. Technical level related threats, how they form and how they can be dealt with have been intensively covered in the literature.

We have compiled a listing of prominent and not so prominent threats at the technical level in Table 2. While many of these items therein are discussed in the literature already cited, items not discussed in the literature, are also included to make this a more comprehensive list of threats.

THREATS RELATED TO FORMAL ASPECTS

Threats related to procedures, regulations, governance, rules and policies

Security threats can be managed through policies that set up rules for employees and programs to increase education and awareness about threats (Whitman and Mattord, 2008). The success of such policies is tied to several factors among which: management support identification of security threats, distribution of policy to employees, ensure proper understanding of security requirements through training, ensure that the security policy reflects the business objectives, and establishment of performance evaluation of security management that provide timely feedback further improvement (Doherty and Fulford, 2006). In this context it should be mentioned that security policy should set the security roles, responsibilities, authorized and prohibited use of

information as well as addressing the requirements for security management (Whitman and Mattord, 2008).

Table 2 Threats at the technical level

Threats at Technical Level		
• Malicious Ware	• Spam	• Outside network connection
• Phishing	• Web transaction	• Traffic flow analysis
• Hardware failure	• Network failure	• Network attack,
• Software and HW crashes	• Loss and destruction of data	• Data interruption
• Service interruption	• Security gateway	• Impersonation
• Technological obsolescence	• Power and Wan service	• Outside web connection
• People	• Communication Protocol	• Traffic flow
• Backup resources	• Service delay	• Connection flooding
• Communication security	• Eavesdropping	• Hardware theft,
• Uncontrolled user privilege	• Physical security	• Interception
• Pharming	• Mirrored servers	• Loss of portable devices
• Sniffers	• Loss due to inadequate	• Lack of Host intrusion detection
• Denial of services and	• Deviation of quality of	• Software bugs
• Distributed denial of services	• Timing attack	• Lack of network intrusion
• Cyber terrorism	• Spoofing	• Lack of physical security
• Encryption/decryption	• Power irregularities	• Improper disposal of used
• IP device	• Misuse of infrastructure	• Absence of server and data backup
• Cyber espionage	• Phreaking	• Wire taping
• Mobile computing issues	• Cloud computing	• Operation accidents
• Mirror server	• Power outage	• Sabotage
• Lack of IT auditing dimension	• Lack of training	• Incompetence
• Email	• Exploited vulnerability	• Unauthorized software
		• Lack of compliance monitoring

Several studies covered the topic of information security policy where researchers were able to identify the success factors that influence policy, however, none of the research showed how to effectively design an easy to communicate clear and well written policy that can be equally applied by both business managers and IT managers. Anderson (2007) showed that there is a discrepancy between the level of implementation of security policy between business managers and IT managers. This, as a result, forms a managerial challenge within the organization and becomes more intense when dealing with other organizations. Absence of processes and procedures increases the vulnerability of the information system and increases the level of risk the firm may encounter.

We have compiled a listing of prominent and not so prominent threats at the formal level in Table 3. While many of these items therein are discussed in the literature already cited, many items, not discussed in the literature, are also included to make this a more comprehensive list of threats.

Table 3 Threats at the formal level

Threats at Formal Level	
• Miscommunicating	• Conflicting procedures
• Document control, release, and effective date	• Procedures are hard to comply with
• Lack of training	• People
• Vague access rights	• Managed users
• Deliberate act of theft	• Managed devices
• Conflicting rules	• Authentication
• Over bureaucratization	• Absence/deficiency of transaction logs
• Absence of procedures	• Need for data and idea sharing
• Accountability	• Repudiation
• Socio political issues	• Unavailability threat
• Access control	• Legal
• Integrity threat	• Absence of Published standard
• Confidentiality threat	• Lack of incident reporting and investigation procedures
• Elevation of privilege	
• Authorization	

People as a Threat to Information Security at The Different Managerial Levels

As can be seen and discerned from the daily activities of different organizations, a common factor that influences each of the three threat categories, that were formerly addressed, is people. People are the main focus of the informal threat category that are basically people related in terms of behavior, attitude, awareness, perception, motivation, culture and training.

People form a source of both internal and external threat. According to Wilson and Zviran (1992) "Threats from insiders, authorized to use the computer system, can be categorized as mistakes, dishonest employees with self-serving goals, loss or disruption to computer systems from any cause, and disgruntled employees who commit damaging acts without economic or other self-serving goals." Keller et al. (2005) reported that 55.6 % of the medium sized companies they surveyed (<500 employees) acknowledged internal personnel as the primary source of threat.

Waxer (2007) referred to three major employee related threats: (1) employees unintentionally giving out the company information, (2) employees losing their laptops, and (3) spreading information through unsecured emails. Colwill (2009) stated that insiders are more of a threatening factor than outsiders to the firm because they can possibly harm the system in a repetitive way due to the fact that they have lawful and privileged access to information. Besides, insiders are always more aware of the organization input, output and its crucial assets. The author mentioned that many technological aspects, like firewalls and intrusion detection system, are available to protect information supported by different procedures and guidelines to avoid outsider people attacks that are easy to detect and defend. Authors like McCue (2008) claimed that 70 % of fraud activities come from insiders however 90 % of the security controls focus on the outsider.

McAfee (2008) discussed how economic recession has lead to increased rate of cybercrime because employee feel threatened by downsizing that took place in many firms in order to cut costs. Threats that come from insiders (employees) can be understood using the congruence model developed by Wyman (2008) which focuses on the cultural factors that may influence threats coming from "within the organization." In the congruence model, Wyman (2008) referred to the process transformation elements as: work, people knowledge and skills, formal organization and informal organization values, beliefs and culture. The author mentioned that the performance of organizations depends on the degree of fit between work, people, structure and culture. In that sense, thinking of information security threat model should consider those elements alongside with the technical element.

In addition to the "insiders threat", people from outside can also form "outsider threat" or "hackers" who try to penetrate a computer system. Also, there is another source of outsider threat called 'crackers' who are malicious hackers and are comprised mostly of juvenile delinquents, who are a serious nuisance for business (Wilson et al., 1992).

Managers should be able to identify the weakness in employee practices which constitute the biggest threat to an organization's information (Rhee et al., 2009). Therefore, the biggest challenge to information security professionals is to know how to reposition people from being the biggest source of vulnerability to the first line of defense (Moore, 2003). Managers should put effort to ensure that IT users realize how information security threats can bring dangerous consequences that could be avoided by committing to security practices (Huang et al., 2011).

THREATS RELATED TO INFORMAL ASPECTS

Information Security Awareness

Among users, lack of awareness about security policies and best security practices has been recognized by scholars as a major cause of system failure (Siponen, 2000). Siponen (2001) identified four dimensions of IS awareness: (1) general public dimension that is needed to inform ordinary computer users about the risks related to use of information technology, (2) socio-political dimension, (3) computer ethical dimension, and (4) the institutional education dimension that should go hand in hand with computer ethical dimension to enhance the awareness of computer ethics. Securing information entails increasing the awareness level on the four dimensions by providing awareness training and updates for the different users to cope with the changing nature of threats. Such training programs should not only be provided when the users first start using the technology. Rather, progressive and reinforcement training should be provided from time to time to the different users in order to remain up to date with the changing environment (Abraham and Michie, 2008).

Information Security Perception

Perception is a major constituent of human intelligence and is important to understand human behavior (Salvendy, 1997). Cooper (2003) It is the way for people to evaluate external inputs that influence the behavioral response (Cooper, 2003). People respond to different kinds of threats according to their perception. Overestimating the threat may hinder the use of information technology (Featherman and Pavlou, 2003; Lim, 2003; Suh and Han, 2003; Pikkarainen et al., 2004; Jih et al., 2005; Yang, 2005; Yenisey et al., 2005), for example, e-banking may not be used at all because of security problems. On the other hand, underestimating the threat may lead people to involve in insecure practices (Stewart, 2004; Thomson and Solms, 2005; Chai et al., 2006) exposing themselves and their organizations to different kinds of problems. Huang et al. (2010) prudently emphasized that what people perceive, why they have a certain perception, and the resulting behavior need to be investigated as part of the human factors that influence and impact information security.

Motivation Towards Information Security Behavior

Lack of motivation towards information security behavior may lead people to not apply security policies and guidelines which in turn form a source of threat to the information security (Leach, 2003). In order to motivate people towards security behavior, we need to influence their perception of risk by educating them about the different types of risks and their consequences (Fischhoff et al., 1978).

People can be motivated toward information security behavior through rewards. Motivation towards security behavior can be increased by rewarding employees and by giving them the chance them to be socially involved in dealing with security issues (Ruighavar et al., 2007)

Culture

Finne (1996) pointed out the importance of building a strong information security culture within a company. The author stated that "a company with gaps (mostly unplanned) in its culture on information security issues will most probably have Information Security (ISEC) breaches, which will have significant influences on the functions of the company. Thus, the employees have to take their responsibility for the company's ISEC."

Schein (2004) defined group culture as:" a pattern of basic shared assumptions and internal integration, that was well worked enough to be considered valid and, therefore, to be taught to new members as the correct way to perceive, think and feel in relation to those problems." Managers should be aware of both language and norms when trying to build the information security culture especially when that culture need to be spread within globalized firms that are geographically scattered (Colwell, 2009).

We have compiled a listing of prominent and not so prominent threats at the formal level in Table 4. While many of these items therein are discussed in the literature already cited, many items, not discussed in the literature, are also included to make this a more comprehensive list of threats.

Table 4 Threats at the informal level

Threats at the Informal Level	
• Social networking	• Misinformation
• Loss of cell phones and laptops	• User role vulnerabilities
• Misuse	• Manager role vulnerabilities
• Employees daily activities and behavior	• Social norms
• Intentional data distortion by employees	• Lack of motivation toward security behavior
• Disclosure of information	• Social Engineering
• Disgruntled employee	• Shoulder surfing
• Termination of employment procedures	• Tampering with data
• Absence of "ownership"	• Consumerization of IT
• Lack of "sense of belonging"	• People (i.e Business partner, contractors, consultant,
• Lack of awareness	• Not following the rules
• Poor supervision	• Inappropriate activity (Intentional, Unintentional)
• Cultural issues (language, ethics, morality)	• Insecure business contractors
• Legal issues	• Piecemeal gathering of information
• Pay scale relative to "responsibilities"	• Discard the info on work paper
• Absence of Public Awareness	• InfoSec perception
• Employee misperception about the threat	• Lack of training
• Limited human resource	• Lack of awareness program
• Sabotage	• Lack of training and relevant communication
• Espionage	• Carelessness

MANAGEMENT CONTROL

Management control is intended to evaluate the effectiveness of the measures taken towards achieving the security of information by: (1) identifying the information system, defining its criticality, and how they contribute to the creation of business value (Raggads, 2010); (2) identifying all threats, assessing them and taking the necessary corrective and preventive actions; and (3) continually improving the security programs to cope with system dynamics. Raggads (2010) stated that "managerial controls focus on the management of information system and the management of risk for a system. They are techniques and concerns that are normally addressed by management. The following are managerial security controls: risk assessment, planning, system and system acquisition, and certification, accreditation, and security assessment."

Managers should prepare themselves to the complexities of applying a holistic information security program that controls for the technical, formal and informal aspects of the threats. In addition, they should be cognizant about the challenges they may face in doing so. Some of these challenges were discussed by Dhillon (2001) as: (1) establishing good management practices in the multicultural environments, (2) establishing policies and procedures that match the organizational context, (3) establishing proper structural responsibility, (4) establishing appropriate recovery plans for the system.

To these challenges, we would like to add another two challenges. The first is the challenge of business continuity under all conditions, and the second is the challenge of managing the changes that take place within the system.

Based on the facts that 55.6 % of medium size companies acknowledge internal personnel as a main source of threat, and 70 % of fraud activities come from people from inside the organizations (McCue, 2008), a framework for managing threats is proposed in this paper. The logic for our proposed framework will be centered around people as the first line of defense that should receive significant attention for achieving system and information security. In this regard, the most important and influencing task would be to cultivate the information security culture among people as they represent the major resource necessary for establishing technical and non-technical information security environment.

Thus, setting information security principles through the organizational culture should come first in the threat control framework as indicated in Figure 1. This, in turn, influences the perception about information security. That "InfoSec perception" will shape attitudes toward performing a certain security act. Attitude, as a result, influences intention to comply with policies and procedures governing the information security.

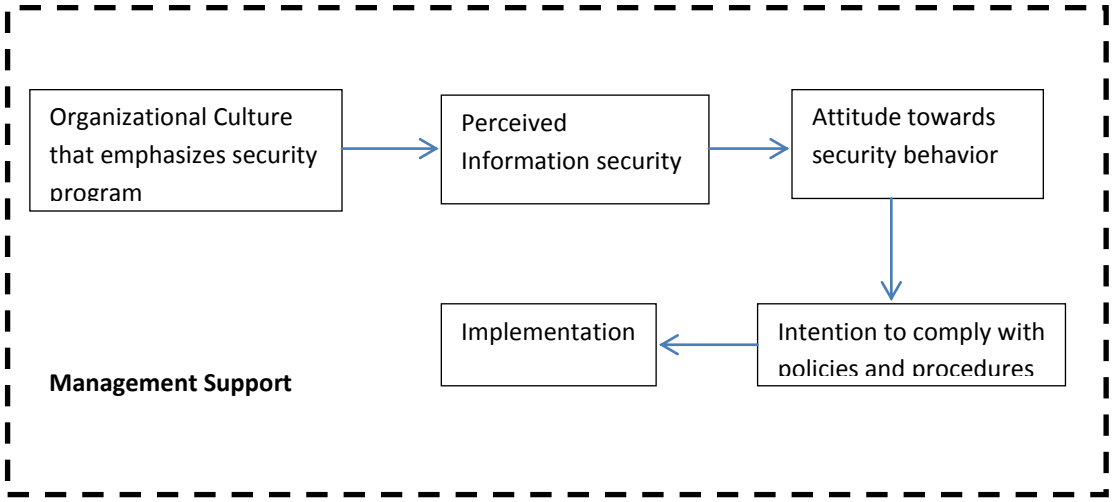

Figure1 Information security success model

We believe that managing the inter-organizational aspect can be reinforced through "Information security standardization or following international best practices for information security management" (Solms, 2000).

Cautious managers should always implement metrics to continuously and dynamically measure information security aspects within his organization and between organizations within the supply chain.

References

References available upon request from: Elsaleiby Aber: Aber.Elsaleiby@rockets.utoledo.edu, Kunnathur Anand: Anand.Kunnathur@utoledo.edu