THREATS AND COUNTERMEASURES OF THE REALM IN 2011

Joseph H. Schuessler
Tarleton State University,
Box T-0170,
Stephenville, Texas, U.S.A. 76402
E-mail: schuessler@tarleton.edu

ABSTRACT

Information Systems Security (ISS) is of primary concern to organizations for a variety of reasons including mounting requirements for regulatory compliance in the wake of financial scandals, growing dependence on information systems to provide the backbone of organizational structures, and rising organizational dependence on ecommerce to conduct daily activities. However, despite ISS being largely a managerial issue, managerial concern for ISS is still inadequate, evidenced by its consistently low ranking as a key issue in information systems management surveys.

This research seeks to examine the dynamic nature of threats and countermeasures by examining prior research on the subject and comparing the results of that research to contemporary results. Results suggest that, based on interview responses from experts, both threats and countermeasure responses have changed over time. Interpretation of the results will help practitioners to better understand modern threats and potential remedies to address them.

INTRODUCTION

The growing importance of Information Systems Security (ISS) for organizations has occurred for numerous reasons including the mounting requirements for regulatory compliance in the wake of financial scandals (Abu-Musa, 2004), growing dependence on information systems to provide the backbone of organizational structures (Kankanhalli et al., 2003), and rising organizational dependence on ecommerce to conduct daily activities (Barsanti, 1999). However, despite ISS being largely a managerial issue (Hitchings, 1995); managerial concern for ISS is still inadequate, evidenced by its consistently low ranking as a key issue in information systems management surveys (Ball and Harris, 1982; Dickson et al., 1984; Brancheau and Wetherbe, 1987; Brancheau et al., 1996; and Pimchangthong et al., 2003; Luftman and Ben-Zvi, 2010). This has led some researchers (Dhillon and Backhouse, 2000) to call for greater concern from management in order that they may fully appreciate the need for effective ISS and become aware of the salient issues.

Each industry is faced with a unique set of threats for which a unique combination of countermeasures is appropriate (Straub and Welke, 1998). The dynamic nature of threats and as a result, appropriate countermeasures make periodic review of each necessary. The dynamic nature of each can be seen by examining prior studies on the subject and observing the changing importance of various threats and countermeasures. The identification of the changing nature of threats and countermeasures can be used to identify trends and promote more proactive, efficient, and effective responses to threats.

LITERATURE REVIEW

Interest in ISS has existed for some time but it has remained relatively low on the radar of many practitioners until relatively recently. This can be seen by examining the numerous studies over the years in which top management has fluctuated over the importance of ISS. For example Loch et al. (1992) noted that in 1981, ISS ranked 14th among management's concerns. By 1985 concern for ISS had moved up to 5th. However, by 1989 it had fallen back down, this time to 19th as an issue of concern for management. More recently in 2003, ISS was ranked 17th in developed countries (Pimchangthong et al., 2003). This is of particular concern given the heightened emphasis in the wake of the September 11th, 2001 events. Though ISS began to gain steam in 2007 in terms of importance (Luftman and Kempaiah, 2007), it seems to have been derailed by fiscal pressures to reduce costs in light of the global economic issues experienced (Luftman et al., 2008; Luftman and Ben-Zvi, 2009; Luftman-Ben-Zvi, 2010). When put into context with respect to the top concerns for management, it can be seen that while the focus on security has fluctuated in its importance, it has never consistently been considered to be of strategic importance. In 1989, Hoffer and Straub pointed out that legislators have paid more attention to security issues than practitioners by passing legislation at state and federal levels. More recently, acts such as the Sarbanes-Oxley Act of 2002 (SOX) serve to illustrate that perhaps legislators are still more proactive with respect to security than practitioners. Acts such as SOX often have far reaching effects in that they often are designed to correct or regulate a particular issue but have unforeseen consequences in seemingly unrelated areas. SOX in particular may be considered more surreptitious in that it dictates to public firms that they must attest to the accuracy of their financial records but gives little guidance with respect to how to secure records and properly implement policies. In order for an organization to comply, they must have established policies and controls in place in order to be able to document the soundness of their security implementations. However, in order to develop appropriate policies and controls, a comprehensive understanding of the threats faced by an organization must be understood. The goal of this research is to explore the threats and countermeasures faced by practitioners by first identifying each, ranking them, and then comparing the results to similar studies in the past in order to identify trends.

Threats

Threats represent "a broad range of forces capable of producing adverse consequences" (Loch et al., 1992, p. 174). Therefore, a threat creates risk by creating the capability, or probability, that a force will act, in the context of information systems, adversely on an information system. One of the aspects of threat analysis that makes it so difficult is that it can be viewed from multiple dimensions: internal/external, human/non-human, accidental/non-accidental, and so on (Loch et al., 1992). While this classification scheme provides an intuitive way for practitioners to classify threats, the dimensionality adds to the complexity when attempting to determine the most appropriate mix of countermeasures to be used. Loch et al. (1992) and Whitman (2004) illustrated numerous threats to information systems including natural disasters, access of systems by competitors, inadequate control over media, to name a few. Threats are also dynamic in the sense that they constantly change over time to adjust to the various countermeasure techniques used to combat them and as technology changes as well. As an example of the dynamic nature of threats, one need only examine the weighted ranks of threats between the Loch et al. (1992) study and the study conducted by Whiteman (2004). See Table 1 for a side-by-side comparison and mapping of the threats from Loch et al. (1992) to Whitman (2004). In the Loch et al. (1992) study, it was found that the entry of a computer virus only ranked fifth. By 2004, Whitman found that deliberate software attacks had risen to number one. There could be a semantic argument in terms of the definition of "deliberate software attack" versus "entry of a computer virus" but the nature of each threat is similar. Similarly, Natural disasters had dropped from the greatest threat in 1992 to eleventh in 2004. The dynamic nature of threats is likely caused by dynamic business environments, technology changes, hacker motivations, and so on.

Table 1: Comparison of Weighted Threat Rankings in IS

Loch et al., 1992		Whitman, 2004	
Entry of Computer Viruses (E)	5	Deliberate Software Attacks	1
Poor Control of I/O (I)	9	Technical Software Failures or Errors	2
Accidental Entry Bad Data by Employees/Accidental Destruction Data by Employees(I/I)	2/3	Act of Human Error or Failure	3
Access to System by Hackers Access to System by Competitors (E/E)	6/12	Deliberate Acts of Espionage or Trespass	4
Intentional Destruction Data by Employee/Intentional Entry Bad Data by Employee (I/I)	10/11	Deliberate Acts of Sabotage or Vandalism	5
Inadequate Control Over Media (I)	7	Technical Hardware Failures or Errors	6
		Deliberate Acts of Theft	7
Natural Disasters (E)	1	Forces of Nature	8
Access to System by Hackers Access to System by Competitors (E/E)	6/12	Compromises to Intellectual Property	9
		Quality of Service Deviations from Service Providers	10
		Technological Obsolescence	11
		Deliberate Acts of Information Extortion	12
Weak/Ineffective Controls (I)	4		
Unauthorized Access by Employees (I)	8		
Other Threats	13		

Countermeasure Efforts

"Modifying factors" (Loch et al., 1992) which represent internal and external forces that can influence whether or not a threat is able to be realized and/or affect the severity of such a threat if it were to occur are referred to as "counter-measures" (Schultz, 2004; Straub and Welke, 1998;

Whitman, 2004; Hill and Smith, 1995; Hoffer and Straub, 1989). Countermeasures are used by organizations in order to influence the effect that a threat has on their information systems in order to reduce risk and increase ISS effectiveness (Madnick, 1978; Kankanhalli et al., 2003). For each risk, there is one or more corresponding countermeasure(s) available in order to mitigate the threat from being realized (Madnick, 1978). Mitigation is intended either to eliminate the threat all together or to limit the impact of the threat such that risk is reduced. Ultimately, countermeasures are designed to reduce risk by mitigating the probability and severity of realized threats and to protect information system assets. While threats can exist without risk, risk cannot exist without a corresponding threat to potentially carry out an action.

This research drew heavily on prior research to establish a theoretical lens appropriate for analysis of countermeasures. General Deterrence Theory (GDT), a theory originating from the field of Criminology and extensively applied in the area of ISS by, among others, Straub and company (Straub, 1986; Nance and Straub, 1988; Hoffer and Straub, 1989; Straub and Nance, 1990; Straub and Welke, 1998), was used as a way to categorize and classify various countermeasures that an organization has at its disposal. The theory consists of four dimensions (deterrence, prevention, detection, and remedy) and provides practitioners a theoretically based perspective with which to implement countermeasures. Deterrence can proactively dissuade potential violators from implementing a threat by warning them about logging policies and warning of remedial actions. Prevention also proactively seeks to protect information systems by hardening potential targets through use of firewalls, anti-virus solutions, and so on. Detection is a reactive approach that aids in the identification of perpetrators should a threat be attempted. Active and effective detection techniques can aid deterrence efforts by promoting both the ability and likelihood of catching violators. Similarly, remedy efforts can also aid in future deterrence efforts by providing clear-cut means of doling out punishment for various infractions upon an information system. Like detection, remedy efforts are reactive in the sense that they are in response to an event that has already occurred.

The Loch et al. (1992) study focused on threats and did not assess countermeasures. Because of the inability of a single data point to illustrate trends, the rankings for an organization's use of countermeasures are not provided here. It is provided below in Table 4 in order for comparisons to be made with the data collected in this research.

METHODOLOGY

Burns and Grove (2004) identified three sources of content validity: (1) literature, (2) representativeness of the relevant population, and (3) experts. Ultimately, the determination of whether or not an instrument contains content validity is subjectively based on the opinions of experts (Nunnally, 1978). As a result, the current research sought the opinions of "experts" in positions that required both a technical and managerial understanding of the threats and countermeasures used in information systems. Six practitioners with titles such as "Computer Systems Manager", "Information Systems Technical Manager", and "Network and Systems Manager" were identified from a convenient sample for interview. Each interview was recorded to a digital recorder and included some written responses in order to obtain the classification information. Each individual referred to their role as being more managerial rather than technical though two specifically mentioned more of a balance between the two extremes. Further demographics of the interviewees can be seen in Table 2 below.

Table 2: Interviewee Demographics

	Interviewee					
	1	2	3	4	5	6
Years with organization?	9-16	17-24	25+	9-16	9-16	9-16
Years in current position?	9-16	9-16	25+	9-16	9-16	9-16
Managerial versus Technical in nature?	Managerial	Managerial / Technical	Managerial	Managerial	Managerial	Managerial / Technical
Years of experience in IS?	20	16	32	19	9	30
Years of experience where security issue were a main component of that experience?	12	6	32	3	9	25

Using structured interviews with open ended-questions, a grounded theory approach was used in order to obtain rich responses that are more difficult to obtain using traditional survey methods. The open-ended questions were guided using the framework put forth by Loch et al. (1992) by first defining each dimension (internal-external, intentional-unintentional, human-nonhuman) and then asking the interviewee about the type of threats faced by their organization. After each of the open-ended questions had been answered, each interviewee was presented a table which listed each threat identified by Whitman (2004). The respondent was then asked to identify the origins of each threat along the dimensions identified by Loch et al. (1992).

Countermeasures were identified similarly. Using GDT, each dimension was defined in the interview process. Respondents were asked then to identify various countermeasures their organization used relative to each dimension. Threats identified by Whitman (2004) were used as a starting point for the interviewees. Upon completion of the structured interviews, they were again presented a list of threats identified with Whitman (2004) and asked to identify and additional threats their organization faced. Once complete, they were asked to rank and classify the threats their organization faced.

DATA ANALYSIS AND RESULTS

To analyze the data collected in the process, digital recordings of each interview was transcribed to a rich text file format. Each file was then imported into Max QDA, a Qualitative Data Analysis software package, used to code and interpret data. Max QDA has been successfully used in data analysis in the social sciences (Randall, 2007; Sharp 2009) and is an accepted analysis tool. Using the framework for threats identified by Loch et al. (1992), text segments were coded for each interview. This allowed for a comprehensive identification of relevant threats faced by the group of respondents.

In order to identify a clear ranking across all respondents, each threat was input into a spreadsheet along the left column, each on its own row. Each respondent was represented across the top of their respective columns. Their rakings were input into the appropriate cells. Once all values were entered into the spreadsheet, averages for each threat were generated in order to be able to identify those with higher and lower averages and thus consensus rankings. The results of these rankings and comparisons to both Loch et al. (1992) and Whitman (2004) can be seen in Table 3 below.

Table 3: Comparison of Weighted Threat Rankings in IS

Loch et al., 1992		Whitman, 2004		Schuessler, 2011	
Entry of Computer Viruses (E)	5	Deliberate Software Attacks	1	Deliberate Software Attacks (viruses, worms, macros, denial of service)	1
Inadequate Control Over Media (I)	7	Technical Hardware Failures or Errors	6	Technical Hardware Failures or Errors (Equipment Failures)	2
Accidental Entry Bad Data by Employees/Accidental Destruction Data by Employees(I/I)	2/3	Act of Human Error or Failure	3	Act of Human Error or Failure (accidents, employee mistakes)	3
Natural Disasters (E)	1	Forces of Nature	8	Forces of Nature (Fire, Flood, Earthquake, Lightning)	4
Access to System by Hackers Access to System by Competitors (E/E)	6/12	Compromises to Intellectual Property	9	Compromises to Intellectual Property (piracy, copyright infringement)	5
		Quality of Service Deviations from Service Providers	10	Quality of Service Deviations from Service Providers (Power and WAN Quality of Service Issues)	6
		Deliberate Acts of Theft	7	Deliberate Acts of Theft (Illegal Confiscation of Equipment or Information)	7
Intentional Destruction Data by Employee/Intentional Entry Bad Data by Employee (I/I)	10/11	Deliberate Acts of Sabotage or Vandalism	5	Deliberate Acts of Sabotage or Vandalism (Destruction of Systems or Information)	8
Access to System by Hackers Access to System by Competitors (E/E)	6/12	Deliberate Acts of Espionage or Trespass	4	Deliberate Acts of Espionage or Trespass (unauthorized access and/or data collection)	9
Poor Control of I/O (I)	9	Technical Software Failures or Errors	2	Technical Software Failures or Errors (Bugs, Code Problems, Unknown Loopholes)	10
		Deliberate Acts of Information Extortion	12	Deliberate Acts of Information Extortion (Blackmail of Information Disclosure)	11

				Social Engineering	12
		Technological Obsolescence	11	Technological Obsolescence (Antiquated or Outdated Technologies)	13
				Pandemics	14
Weak/Ineffective Controls (I)	4				
Unauthorized Access by Employees (I)	8				
Other Threats	13				

In a similar fashion, countermeasures were also input into a spreadsheet and average rankings identified. The relative rankings can be seen below in Table 4.

Table 4: Countermeasure Rankings

Whitman, 2005		Schuessler, 2011	
		Password Policy	1
		Physical Area Security	2
Employee Education	4	Employee Education	3
Use of Passwords	1	Use of Passwords	4
Firewall	7	Firewall	5
Virus Protection Software	2/3	Virus Protection Software	6
Media Backup	2/3	Media Backup	7
Consistent Security Policy	6	Consistent Security Policy	8
Audit Procedures	5	Audit Procedures	9
Publish Formal Standards	11	Publish Formal Standards	10
Control of Workstations	12	Control of Workstations	11
Host Intrusion Detection	14	Host Intrusion Detection	12
Ethics Training	15	Ethics Training	13
Network Intrusion Detection	13	Network Intrusion Detection	14
Monitor Computer Usage	10	Monitor Computer Usage	15
Auto Account Logoff	9	Auto Account Logoff	16
Encourage Violations Reporting	8	Encourage Violations Reporting	17
No Internal Internet Connections	18	No Internal Internet Connections	18
No Outside Network Connections	19/20	No Outside Network Connections	19
No Outside Web Connections	21	No Outside Web Connections	20
No Outside Dialup Connections	16	No Outside Dialup Connections	21
Use Shrink-Wrap Software Only	17	Use Shrink-Wrap Software Only	22
Use Internally Developed Software Only	19/20	Use Internally Developed Software Only	23

DISCUSSION

The results above can help practitioners identify the most significant threats faced by organizations as well as available countermeasures used to combat such threats. For example, it can be seen by examining the threats faced by organizations that deliberate software attacks continues to be the top issue faced by practitioners. This is likely the result of continued integration of systems to online environments and the shifting of motives in hacking attempts from that of mere exploration or the thrill of breaking in to the more monetarily lucrative aspect of stealing identities, credit card numbers, corporate espionage, and so on.

But, technical hardware failures and equipment failures has risen to the second highest threat faced by organizations. This may have something to do with the budgetary constraints faced by many organizations over the last few years leading to an inability to replace aging equipment (Matzke and McCarthy, 2008).

Act of human error or failure continues to rank third since Whitman's (2004) study. This only reaffirms the symbiotic relationship we as individuals still have with information systems; from accidentally inputting data to improper configuration of hardware and software. Human error continues to plague information systems managers (Laudon and Laudon, 2012).

Forces of nature as a threat are back on the rise. This is likely due to the major environmental events that occurred since the Whitman (2004) study (i.e. Hurricane Katrina and pandemics such as the Bird Flu epidemic). Two respondents mentioned pandemics by name as a concern and discussed the issues related to running their departments under such circumstances from remote locations. Though it could be argued that this should fall under the natural disasters categorization, one respondent drew a clear distinction between the two.

Compromises to intellectual property were also identified as being on the rise as a concern of the interviewees. Of particular concern was the adherence to license agreements, making sure that employees were using valid installations of software installations. One respondent, operating in an environment where users may provide their own software, stated that they attempt to verify the adherence to software licenses, but that the problem is difficult because there were so many nuances to each agreement.

Limitations of the Study

As with all studies, this study is subject to limitations, which can potentially influence conclusions drawn from the dataset. First, because an interview process was to for data collection, this necessarily limited the number of data points. Interviews were necessary in order to obtain such rich response but this limits the generalizability of the study and as a result, conclusion drawn from the study should keep this in mind.

The lack of a common definition of terms makes it difficult to compare the results of one study to another. For example, it became apparent in the interview process when respondents were asked about the use of passwords, that a subtle distinction was apparent: the simple use of passwords versus password policies which affect the frequency of change and password complexity. This lack of continuity makes it difficult to measure and compare the rankings of various threats and countermeasures over time. The use of different definitions likely plays a role in this as does the dynamic nature of threats and as a result, countermeasures which results in the need for new consideration in the meaning of terms over time.

Research Contributions and Implications

This research extends our understanding of the trends associated with threats and countermeasures. Such an analysis is necessary in order to obtain a true picture of the phenomena. By understanding the trends associated with threats and countermeasures, researchers can focus their efforts on developing appropriate risk assessment strategies for high priority threats and the effectiveness and identification of appropriate countermeasures.

Practical Implications

Practitioners can use these rankings of threats and countermeasures in their current risk assessment activities. By identifying the top threats faced by organizations, they can focus their efforts on protecting their systems from these top threats using the myriad of countermeasures identified in the study. The result should be a more efficient allocation of the firm's resources while maintaining effective controls.

Directions for Future Research

The dynamic nature of threats as outlined above make periodic review of threats and countermeasures necessary. Only in this way can the efficient use of resources be applied in the most effective way in order to manage risk. Future research should attempt to standardize the definitions of various terms in order to make comparisons of various rankings more meaningful. Additionally, a consistent methodology should be used for the same purpose. Though the use of interviews limits the number of sources of data, it does provide a very rich dataset from which to draw. It is argued that the richness of the dataset in terms of value is more beneficial than less rich methods such as survey research. Lastly, future research should focus more on the theoretically developed frameworks developed by Loch et al. (1992) and in GDT as a way to classify threats and countermeasures as distinctive classes or dimensions in order to make broader generalizations and more easily understood by decision makers in organizations that do not necessarily have technical backgrounds and understanding of the salient issues of information systems security.

REFERENCES

References are available upon request from Joseph H. Schuessler at schuessler@tarleton.edu.