Information Systems Management, 26: 2–12
Copyright © Taylor & Francis Group, LLC
ISSN: 1058-0530 print/1934-8703 online
DOI: 10.1080/10580530802384639

Information Security Threats: A Comparative Analysis of Impact, Probability, and Preparedness

Mary Sumner
Southern Illinois University Edwardsville, Edwardsville, Illinois

Abstract *The objectives are: (1) to determine the risk assessment of information security threats, based upon the perceived impact and the perceived probability of occurrence of these threats; (2) to determine the extent of risk mitigation, based upon the perceived level of preparedness for each of these information security threats; and (3) to determine the extent to which the of occurrence and the impact of information security threats relate to the level of preparedness.*

Keywords information security, risk assessment, risk mitigation

Theoretical Framework: Risks and Mitigation Strategies

In 2002, the Computer Security Institute/FBI conducted a survey on computer crime and security. The majority of those who responded were government agencies and large corporations, and 90% of them had detected a computer security breach in the past year (Whitman, 2003).

Information security threats are risks that need to be managed. A risk is defined as “the possibility of an event occurring that will have an impact on the achievement of objectives. Risk has two components: the probability/likelihood of failing to achieve an outcome and the impact/consequence of failing to achieve that outcome” (Defense Systems Management College, 2001). In another definition, “risk is a financial measure of the impact of a failure x the probability of an event occurring” (Stoneburner, 2006). The ability to assess risks is the first step in risk management. Risk assessment is the *process* of assessing the impact of information security threats and the probability that these information security threats will occur. Risk mitigation is the process of developing preventative strategies to minimize these risks.

Risk management should be taken seriously due to criticality and cost. Organizations want to safeguard against high-impact, high-probability risks because of their consequences, and they should be able to invest financial resources in controlling these risks. In contrast, it does not make sense for organizations to waste money implementing risk mitigation strategies on low-impact, low-probability risks (Pinto, Arora, Hall, & Schmitz, 2006).

The purpose of this study is to address two issues. First, what is the assessment of information security risks? A risk assessment is based upon an analysis of the impact of information security threats and the probability of their occurrence. Second, what risk mitigation strategies are being used to manage and to minimize these information security risks? The extent of risk mitigation is measured by the level of preparedness of organizations with respect to addressing these information security threats. This study uses the information security threats defined in Whitman’s study (2003).

Ideally, the greater threats (e.g., those with higher impact and higher probability of occurrence) will be addressed through greater levels of risk mitigation designed to minimize the effect of these threats. A lack of alignment between the greater information security threats and the level of preparedness to deal with these threats needs to be understood so that managers can identify effective risk mitigation strategies.

The underlying premise of this study is that risk assessment is a critical strategy in risk management. The study provides a risk management methodology, which includes an assessment of information security threats, based upon an analysis of the perceived impact and perceived probability of occurrence of these threats. The study then determines whether the level of risk mitigation practiced by organizations is aligned with the perceived level of risk.

Address correspondence to Dr. Mary Sumner, School of Business, Professor of Computer Management and Information Systems, Campus Box 1106, Southern Illinois University Edwardsville, Edwardsville, IL 62026, USA. E-mail: msumner@siue.edu

As such, the study demonstrates use of a methodology, which will enable practitioners to develop risk mitigation strategies, which are based upon risk assessment. While this particular study uses the twelve information security threats defined in Whitman's (2003) study, the methodology is reusable and applicable to other risk factors in information security management. The methodology is of value to both academic professionals and practitioners.

Review of the Literature

The review of the literature provides background into the (1) impact of information security threats; (2) the probability of occurrence of information security threats; and (3) the level of preparedness to deal with information security threats. These are the main issues being addressed by this paper.

Impact of Information Security Threats

According to the seventh annual IT survey of over 700 respondents, 80% of whom were chief financial officers, information security issues were ranked as the number one IT issue. Ten percent of the respondents reported at least one business interruption due to security flaws, and five percent reported at least two business interruptions, defined as at least one day of downtime due to a security incident (Sinnett & Boltin, 2006).

The Ernst and Young 2002 Survey reported that the top two causes for the unavailability of critical business systems were hardware or software failure (56%) and telecommunications failure (49%). A high number of failures were due to system capacity issues and operational errors (Ernst & Young, 2002). The CPM/KPMG 2002 Business Continuity Benchmark Survey, based upon 624 respondents, shows comparisons between 1999 and 2002 for business interruptions due to human error, power outage, service provider failure, communications failure, natural disaster, hardware failure, and software failure. In this timeframe, all of these risks were prevalent, and the only risk, which decreased in importance, was risk from natural disasters (Hagg, 2002).

The Ernst and Young 2003 Survey reveals a higher recognition of information security threats, with a major virus or worm perceived as the highest intensity threat, recognized by 77% of the respondents. Employee misconduct with information systems was rated next highest, by 57% of the respondents (Ernst & Young, 2003). The cost of viruses and other computer threats can be quantified. For example, Computer Economics (Carlsbad, California) estimates that corporations spent more than $12 billion in 2001 to clean up virus damage (Cerrullo & Cerrullo, 2004).

One of the newest threats affecting information technology is mobile devices. If these mobile devices are not equipped with the proper software to protect their users from viruses and spam, or are not equipped with data encryption, they pose an information security threat (Garretson, 2007). Using WiFi (802.11) in coffee shops, bookstores, restaurants, and campuses opens up the user to information security risks because wireless attack tools can run anonymously, and the user may not even know if they have been attacked (Potter, 2006).

Probability of Occurrence of Information Security Threats

In a study of top security threats perceived by organizations with over 500 employees, the top five threats are (1) deliberate software attacks; (2) technical software failures or errors; (3) acts of human error or failure; (4) deliberate acts of espionage or trespass; and (5) deliberate acts of sabotage or vandalism. Deliberate software attacks are the most frequently reported threats, with "11.5% of the respondents to the study claiming this happened over 100 times per month." Two other threats are acts of human failure or error, with only 24% of companies claiming no attacks, and software failures or errors, with only 30.2% claiming no attack. See Table 1. (Whitman, 2003).

A 2002 CSI/FBI survey found that 90% of respondents detected computer security breaches within the past 12 months. Of these, 80% acknowledged financial losses due to these breaches – a total of nearly $456 million—up $78 million from 2001! (Whitman, 2003).

In Peiro's study of information security threats affecting small and medium-sized companies, 46% of the respondents reported that they had experienced between 1 and 5 information security incidents in the previous 12 months (Peiro, 2005). In another study of current threats to information security within small/mid-sized business (e.g., fewer than 500 employees), over half (55.6%) felt that the primary threats to data came from internal personnel, even though much of this could be accidental (Keller, Powell, Horstmann, Predmore, & Crawford, 2005). This was consistent with 2004 CSI survey that 59% of companies had experienced internal abuse of net access (Gordon & Loeb, 2004).

Internal security threats represent considerable challenges. At the top of the list are employees unwittingly giving out vital company information to people phishing (e.g., *fraudulently acquiring sensitive information by masquerading as a trustworthy entity in an electronic communication*) for information. Other information security threats are employees losing laptops, disgruntled employees' damaging important data systems, and employees' leaking company information through email (Waxer, 2007).

Table 1. Number of Attacks per Month as Reported by Respondents

Number of Attacks per Month	*>100*	*51–100*	*10–50*	*<10*	*None*	*No Answer*
1. Act of Human Error or Failure	5.2%	2.1%	14.6%	41.7%	24.0%	12.5%
2. Compromises to Intellectual Property	1.0%	2.1%	3.1%	25.0%	61.5%	7.3%
3. Deliberate Acts of Espionage or Trespass	4.2%	3.1%	3.1%	20.8%	68.8%	
4. Deliberate Acts of Information Extortion			1.0%	8.3%	90.6%	
5. Deliberate Acts of Sabotage or Vandalism	1.0%		3.1%	31.3%	64.6%	
6. Deliberate Acts of Theft			7.3%	38.5%	54.2%	
7. Deliberate Software Attacks	11.5%	9.4%	14.6%	47.9%	16.7%	
8. Forces of Nature	1.0%		2.1%	34.4%	62.5%	
9. Quality of Service Deviations from Service Providers		1.0%	8.3%	43.8%	46.9%	
10. Technical Hardware Failures or Errors		3.1%	11.5%	51.0%	34.4%	
11. Technical Software Failures or Errors		5.2%	18.8%	45.8%	30.2%	
12. Technological Obsolescence		1.0%	15.6%	21.9%	60.4%	1.0%
Average Responses:	4.0%	3.4%	8.6%	34.2%	51.2%	6.9%

Source: Whitman, 2003.

People-related issues are the weakest link in safeguarding and maintaining information security (Wade, 2004). Loss of laptops and PDA's, failure to password protect these devices, and lack of firewall and virus protection from home computers all pose information security threats that are related to people. Individuals may not even be aware that they are exposing themselves and their organizations to risk.

The client/server environment increases flexibility and functionality but also increases vulnerability to attacks. Ryan and Bordoloi developed a list of 15 threats that occur in a client/server environment. These threats are: "access to data system by outsiders, accidental destruction of data by employees, accidental entry of erroneous data by employees, inadequate audit trails, inadequate or nonexistent logon procedures, intentional destruction of data by employees, intentional entry of erroneous data by employees, loss due to inadequate backup or logs, natural disaster, sharing of passwords, single point of failure, uncontrolled read and/or update access, uncontrolled user privilege, viruses, and weak/ineffective physical control." Their findings indicated that in mainframe environments, the biggest threat was natural disaster. In client/server environments, the biggest threat was viruses and worms (Ryan and Bordoloi, 1997).

The annual Cyber Crime Survey, a survey by the Computer Security Institute taken by a large sample of companies from revenue levels ranging from over $1 billion to firms that earn less than $10 million, indicated that viruses were the cause of the greatest amount of loss in firms, followed by unauthorized access (Roberts, 2005). The cyber-crime outlook suggests that the same security threats of the past several years will continue. Personal computers taken by hackers without knowledge of the end-user will continue to be the number one cyber-crime. Seventy percent of all IT security issues come from the organization's insiders (Cook, 2007).

Level of Preparedness for Information Security Threats

In the earlier-mentioned study of information security threats (Whitman, 2003), the companies responding to the survey noted the protection mechanisms used to address these threats. Password security (100%), media backup (97.9%), use of virus protection software (97.9%), and employee education (89.9%) were extensively used. See Table 2.

Audit procedures (65.6%) and the implementation of a consistent security policy (62.5%) were used to a lesser degree. Yet, with recent legislation, such as the Health

Table 2. Protection Mechanisms

Use of Passwords	100%
Media backup	97.9%
Virus protection software	97.9%
Employee education	89.6%
Audit procedures	65.6%
Consistent security policy	62.5%
Firewall	61.5%
Encourage violations reporting	51.0%
Auto account logoff	50.0%
Monitor computer usage	45.8%
Publish formal standards	43.8%
Control of workstations	40.6%
Network intrusion detection	33.3%
Host intrusion detection	31.3%
Ethics training	30.2%
No outside dialup connections	10.4%
Use shrink-wrap software only	9.4%
No internal Internet connections	6.3%
Use internally developed software only	4.2%
No outside network connections	4.2%
No outside Web connections	2.1%

(Multiple responses possible). Source: Whitman, 2003.

Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley (SOX), and Gramm-Leach-Bliley Act (GLBA), rules and guidelines for information security audit and control help firms practice the necessary steps to protect PII, "personally identifiable information." (Herold, 2006). In Ryan and Bordoloi's survey, the respondents rated their preparedness for information security threats in both mainframe and client-server environments, and the biggest threat that companies were prepared for was the inadequate logon procedure (Ryan and Bordoloi, 1997).

The Ernst and Young Global Information Security Surveys for 2001, 2002, and 2003 provide insight into managers' perceptions of their capabilities to manage information security risks. In the 2001 survey, security breaches by external parties were the biggest concern, yet only 33% of the respondents were confident that they could detect a hacking attack. In 2002, slightly more (40%) were confident that they could detect a hacking attack, but another 40% did not investigate information security incidents. In the 2003 survey, 90% noted the high importance of information security, but 34% rated their organization as less-than-adequate in their ability to determine whether their systems were actually under attack (Ernst and Young, 2001, 2002, 2003).

Small and medium-sized organizations are increasingly using networks, mobile computers, and the Internet as tools to improve their organization's infrastructure. While organizations with between 51 and 100 employees have increased network usage, they have not increased security to match the growth (Peiro, 2005). The majority of small businesses do not have any way of measuring the financial impact of security breaches and may downplay or ignore these events (Peiro, 2005).

Despite the fact that 56% of all participants reported security related incidents in a recent study conducted by the Small Business Technology Institute, 40% of the respondents representing small and medium-sized organizations felt very confident in their information security measures, and an additional 43% of the respondents felt at least somewhat confident in their security measures (Peiro, 2005). Few organizations have a formal security plan, largely because of cost (Wilson, 2007). As a result, they may not know where their problems lie, and they may not be able to measure the impact of security breaches (Peiro, 2005).

In a survey of the steps that small businesses take to protect their computer networks and infrastructure, the use of anti-virus software and firewalls was widespread, but only two-third's of the small businesses interviewed used strong passwords and less than two-third's used automatic patching to assure that critical updates were installed. Among small and mid-sized businesses, internal employees present one of the biggest threats to information security (Keller, et al., 2005). Emergency action plans, including tape backup storage and off-site data storage, were not prevalent among those interviewed.

Preparedness and Strategy

Whereas companies are getting better and better at protecting their systems, many companies do not report that they have had a security breach or a computer crime committed against them (Roberts, 2005). As a result, it is difficult to determine the extent and impact of information security breaches.

Combating information security threats is a challenge for both large and small companies. One of the issues facing all companies is a false sense of security. Management and IT need to work together in order to achieve a "corporate information security solution." Doing simple things, like updating patches to fix security-holes, deters hackers once they determine that there are barriers in place (Atkinson, 2005). Assuming that small size will keep a company safe from hackers is a fallacy (Wilson, 2007).

Based upon a review of relevant literature, an overall preparedness program, designed to protect what already exists within a business plan, is an important business strategy. The preparedness plan should be broken down into physical security, information security, emergency response, crisis management, and business continuity planning. Business continuity planning defines the steps to take once a risk is realized, because no matter how many controls and risk mitigation steps are taken, "you need to have systems and processes in place before something happens." (Atkinson, 2005). Ultimately, preparedness is a strategy that assures that information security supports the achievement of business goals.

Research Methodology

Research Questions

1. To determine the risk assessment of information security threats, based upon the perceived *impact* of these information security threats and the perceived *probability of occurrence* of each of these threats.
2. To determine the extent of risk mitigation, based upon the perceived level of *preparedness* to deal with each of these information security threats.
3. To determine the extent to which the perceived *probability of occurrence* of information security threats and the perceived *impact* of information security threats relate to the level of *preparedness* for dealing with these threats.

The research uses a framework, which applies the probability – impact matrix that was originally developed by the Department of Defense to analyze risks (Defense Systems Management College, 2001). The probability – impact matrix is used to plot the probability that a risk will occur against the impact of the risk event given that it does occur. Typically, probability—impact matrices are 5 × 5 matrices, but they can use other scales. Based upon where a particular risk falls in the matrix, corporate policies should dictate risk mitigation responses. For example, a risk with remote probability and minimal impact may only require monitoring, but a risk with certain probability and catastrophic consequences may require immediate control strategies and intense attention.

Using the probability – impact matrix framework as an analytical tool to assess risk, I developed the *information security risk grid*. See Table 3. In this grid, the highest risk quadrant applies to those information security risks, which have high impact and high probability of occurrence. The moderate risk quadrants pertain to those information security risks, which have high impact + low probability, and those risks, which have low impact + high probability. The low risk quadrant applies to those information security risks, which are low impact and low probability of occurrence. This framework will be used to categorize the levels of risk perceived by respondents in this study.

Questionnaire

A web-based questionnaire, administered through www.zoomerang.com was developed and used to collect data for the survey. The web-based questionnaire was designed to give the respondents an opportunity to address three questions with regard to information technology threats.

1. What is the potential impact of the threat to your organization?
2. What is the probability of the occurrence of each of these threats?
3. How prepared is your organization to deal with the potential threat?

Table 3. Information Security Risk Grid

Probability	
Low impact High probability *Moderate risk quadrant 2*	High impact High probability *High risk quadrant 4*
Low impact Low probability *Low risk quadrant 1*	High impact Low probability *Moderate risk quadrant 3*
Impact	

The respondents were asked to assess the impact, probability, and preparedness of their organizations with respect to the following threats, defined in Whitman's (2003) research:

1. Act of Human Error or Failure (accidents, employee mistakes)
2. Compromises to Intellectual Property (piracy, copyright infringement)
3. Deliberate Acts of Espionage or Trespass (unauthorized access and/or data collection)
4. Deliberate Acts of Information Extortion (blackmail or information disclosure)
5. Deliberate Acts of Sabotage or Vandalism (destruction of systems or information)
6. Deliberate Acts of Theft (illegal confiscation of equipment or information)
7. Deliberate Software Attacks (viruses, worms, macros, denial of service)
8. Forces of Nature (fire, flood, earthquake, lightning)
9. Quality of Service Deviations from Service Providers (power or WAN service issues)
10. Technical Hardware Failures or Errors (equipment failure)
11. Technical Software Failures or Errors (bugs, code problems, unknown loopholes)
12. Technological Obsolescence (antiquated or outdated technologies)

The questionnaire contained four sections. The first section asked respondents to rate the impact of each information security threat to the participant's organization, using a 1 to 7 scale, with 1 meaning "not severe impact: and 7 meaning "very severe impact." The second part asked them to rate the probability of occurrence of each of these information security threats, using a 1 to 7 scale, with 1 meaning "not probable" and 7 meaning "very probable." The third part asked respondents to rate the level of preparedness of the organization for controlling such a threat, using a 1 to 7 scale, with 1 meaning "no measures taken" and 7 meaning "all possible measures taken."

The final part of the survey was simply a demographic. Respondents were asked to provide information on gender, age, educational background, job category, time in the MIS field, and time in their current position.

Sample

The sample included IT 102 professionals within ten organizations representing diverse industries. The organizations participating in the survey represented firms employing MIS interns and MIS graduates of the university.

Table 4. Gender, Age, and Educational Background

Gender	
Male	81%
Female	18%
Age	
20–29	15%
30–39	40%
40–49	32%
50–59	13%
Education	
High School	7%
Associates	15%
Bachelor's	63%
Graduate Degree	13%
Other	2%

The organizations were both large and medium-sized organizations, as defined by number of employees. Five of the organizations were classified as "large" companies (e.g., with over 250 employees) and five organizations were classified as small to mid-sized firms (e.g., with fewer than 250 employees). Fifty-five respondents represented large companies, and 47 respondents represented small and mid-sized organizations.

The IT professionals responding to the survey reported demographic characteristics, including age, gender, and educational background. The majority of the respondents were male (81%), between 30 and 49 in age (72%), and with a bachelor's or graduate degree (76%). See Table 4.

The IT professionals participating in the survey had a variety of IT jobs, including programmer analyst, systems analyst, database analyst, network analyst, technical support specialist, project manager, IT manager, and general manager. The respondents reported the number of years' experience in the MIS field, and the number of years' experience in their current position(s). Approximately 50% of the respondents were in technical support or network technical support roles. Approximately three-quarters of the respondents had less than 10 years' of experience in the MIS field, and the majority (88%) reported less than 10 years' in their current position. See Table 5.

Analysis and Findings

Risk Assessment: Impact and Probability of Information Security Risks

The first objective of the study was to determine the assessment of information security threats, based upon the perceived impact of each of the information security threats and the perceived probability of occurrence of each of these threats. Based upon the respondent data, the mean scores for the impact and the probability of occurrence of each of the information security threats was calculated.

Table 5. Job Category, Time in MIS, Time in Current Job

Job Category	
Technical Support	38%
Network Analyst	11%
Manager	10%
Systems Analyst	9%
IT Manager	6%
Programmer Analyst	5%
Project Manager	4%
Data Analyst	4%
Other	13%
Time in MIS	
< 5 years	40%
6–10 years	32%
11–15 years	11%
16–20 years	4%
> 20 years	9%
N/A	5%
Time in Current Job	
< 5 years	62%
6–10 years	26%
11–15 years	2%
16–20 years	7%
> 20 years	2%

Risk Mitigation: Level of Preparedness

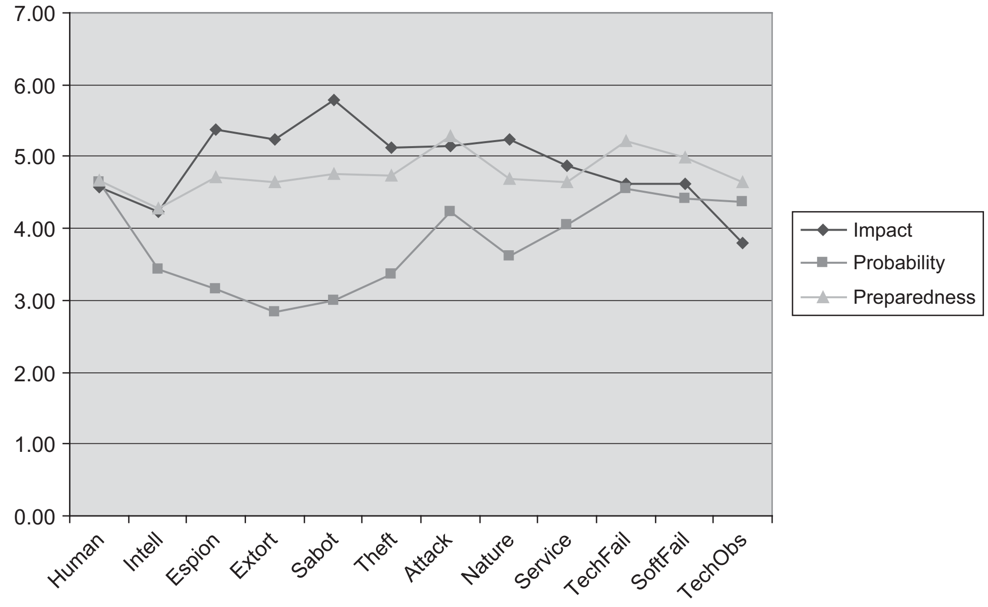
The second objective of the study was to determine the extent of risk mitigation, based upon the perceived level of preparedness to deal with each of the information security threats. Based upon the data, the mean scores for the level of preparedness to deal with each threat was calculated.

See Table 6a for the summary means for the impact, probability of occurrence, and preparedness for each

Table 6a. Impact, Probability, and Preparedness for Information Security Threats

	Impact	*Probability*	*Preparedness*
Legend			
Human Error	4.57	4.65	4.66
Intellectual Property Infringement	4.24	3.43	4.27
Acts of Trespass	5.37	3.15	4.71
Acts of Information Sabotage	5.23	2.84	4.65
Acts of Sabotage or Vandalism	5.79	2.99	4.77
Acts of Theft	5.13	3.37	4.73
Software Attacks	5.15	4.22	5.28
Forces of Nature	5.23	3.63	4.70
Quality of Service Dev.	4.87	4.05	4.65
Tech Hardware Failure	4.63	4.56	5.21
Tech Software Failure	4.63	4.40	4.98
Technological Obsolescence	3.80	4.38	4.63

Table 6b. Graphical View of Impact, Probability, and Preparedness



information security threat. Table 6b provides a graphical view of these data.

Mapping of the Information Security Threats to the Information Security Risk Grid

The third objective of the study was to map the information security threats into the *information security risk grid* in order to identify which risks fell into each of the four quadrants of the grid, including:

The process used to map each of the information security threats into the *information security risk grid* was to use the mean scores of the risk assessment for impact and probability of occurrence of each threat:

Quadrant 4 = High impact (mean > 3.5) + high probability of occurrence (mean >3.5)
Quadrant 3 = High impact (mean > 3.5) + low probability (mean < = 3.5)
Quadrant 2 = Low impact (mean < = 3.5) + high probability of occurrence (mean > 3.5)
Quadrant 1= Low impact (mean < = 3.5) + low probability (mean < = 3.5)

The 3.5 cut-off point was used to delineate high vs. low probability and impact, because it is the halfway point on the 7-point Likert scale, and it is a useful "stroke of pen" to create a partition for analytical purposes. Based upon the impact + probability of occurrence scores, each information security risk was mapped to the *information security risk grid*. See Table 8 for the mapping of each of the information security threats into the *information security risk grid*.

As you can see, a number of information security risks fell into the high-risk (high impact, high probability of occurrence) quadrant. These high-risk information security threats, as perceived by the respondents, included:

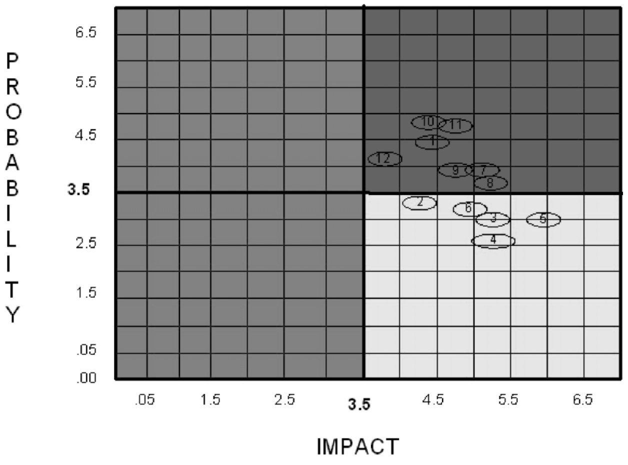
1. Act of Human Error (accidents, employee mistakes)
2. Deliberate Software Attacks (viruses, worms, macros, denial of service)
3. Forces of Nature (fire, flood, earthquake, lightning
4. Quality of Service Deviations from Service Providers
5. Technical Hardware Failures or Errors (equipment failure)
6. Technical Software Failures or Errors (bugs, code problems, unknown loopholes)
7. Technological Obsolescence

Based upon the impact + probability of occurrence scores, additional information security risks fell into the moderate risk quadrant (high impact, low probability)

Table 7. Information Security Risk Grid

Probability	
Low impact High probability *Moderate risk quadrant 2*	High impact High probability *High risk quadrant 4*
Low impact Low probability *Low risk quadrant 1*	High impact Low probability *Moderate risk quadrant 3*
Impact	

Table 8. Mapping of Information Security Risks to the Information Security Grid



1) Act of Human Error or Failure (accidents, employee mistakes)
2) Compromises to Intellectual Property (piracy, copyright infringement)
3) Deliberate Acts of Espionage or Trespass (unauthorized access and/or data collection)
4) Deliberate Acts of Information Extortion (blackmail or information disclosure)
5) Deliberate Acts of Sabotage or Vandalism (destruction of systems or information)
6) Deliberate Acts of Theft (illegal confiscation of equipment or information)
7) Deliberate Software Attacks (viruses, worms, macros, denial of service)
8) Forces of Nature (fire, flood, earthquake, lightning)
9) Quality of Service Deviations from Service Providers (power or WAN service issues)
10) Technical Hardware Failures or Errors (equipment failure)
11) Technical Software Failures or Errors (bugs, code problems, unknown loopholes)
12) Technological Obsolescence (outdated technologies)

1. Compromises to Intellectual Property (piracy, copyright infringement)
2. Deliberate Acts of Espionage or Trespass (unauthorized access or data collection)
3. Deliberate Acts of Information Extortion (blackmail or information disclosure)
4. Deliberate Acts of Sabotage or Vandalism (destruction of systems or information)
5. Deliberate Acts of Theft (illegal confiscation of systems or information)

Risk Mitigation: Level of Preparedness to Deal with Information Security Risks

The fourth objective of the study was to determine the extent to which the perceived impact of each of the information security threats and the perceived probability of occurrence of each of the information security threats was related to the level of preparedness for dealing with each of these information security threats.

The means for the perceived level of preparedness for each information security threat were used to determine the level of preparedness to deal with each threat. See Table 9 for the summary means of preparedness for information security threats.

Five preparedness levels, which were developed to distinguish higher levels of preparedness from lower levels of preparedness. A range was used to identify five preparedness levels. A preparedness level of 5 was aligned with the 90th percentile of preparedness means, or the range of 6.3 to 7.0 on the 1 to 7 scale. A preparedness level of 4 was aligned with mean preparedness scores greater than the 80th percentile, or the range of 5.6 to 6.3 for preparedness scores. A preparedness level of 3 was aligned with greater than 70% percentile range (4.9 to 5.6), a preparedness level of 2 was aligned with greater than a 60% percentile range, and a preparedness level of 1 was aligned with greater than the 50% percentile range (3.5 to 4.2). These distinctions were made in order to compare levels of preparedness for information security risks, which appeared within each of the four quadrants of the *information security risk grid*. See Table 10 for a summary of the preparedness levels used to compare the risk in each of the quadrants in the grid.

The level of preparedness to address each of the information security risks was mapped to each of the four quadrants in the *information security risk grid* to determine if high-risk information security threats are addressed by higher levels of preparedness to deal with these risks. Table 11 includes the data for Impact and Probability associated with each risk, and adds the Preparedness score for each risk.

Table 9. Mean Scores for Level of Preparedness for Information Security Threats

Legend	*Preparedness*
Human Error	4.66
Intellectual Property Infringement	4.27
Acts of Trespass	4.71
Acts of Information Sabotage	4.65
Acts of Sabotage or Vandalism	4.77
Acts of Theft	4.73
Software Attacks	5.28
Forces of Nature	4.70
Quality of Service Dev.	4.65
Tech Hardware Failure	5.21
Tech Software Failure	4.98
Technological Obsolescence	4.63

Table 10. Preparedness Levels

Range	*Percentile Range*	*Preparedness Level*
6.3–7.0	90th	5
5.6–6.3	80th	4
4.9–5.6	70th	3
4.2–4.9	60th	2
3.5–4.2	50th	1

High Impact+High Probability Risks and Level of Preparedness

In terms of the risks in the high impact/high probability of occurrence quadrant, the highest levels of preparedness (level 3) were aligned with the information security risks (7) Software Attacks, (10) Technical Hardware Failures, and (11) Technical Software Failures. (See Table 12). For the high impact/high probability quadrant, lower levels of preparedness (level 2) were aligned with the risks (1) Human Error, (8) Force of Nature, (9) Quality of Service Deviations, and (12) Technological Obsolescence. See Table 12.

Table 12. High-Impact/High-Probability Risks

Higher levels of preparedness	*Lower levels of preparedness*
7, Software Attacks	1, Human Error
10, Technical Hardware Failures	8, Forces of Nature
11, Technical Software Failures	9, Quality of Service Deviations
	12, Technological Obsolescence

Discussion

Reasons for higher levels of preparedness for certain high impact+high probability risks may include the availability of software to protect against software attacks and the availability of technical support tools to guard against technical hardware and technical software failure. Hardware and software technology can be managed and monitored more readily and effectively than the information security threats which require changing the work methods and habits of people.

Reasons for lower levels of preparedness for certain high impact + high probability risks may include the perceived difficulty to address human error, such as accidents and employee mistakes. From the review of the literature, there is an indication that people are the weak link in safeguarding information security, and people may not even know that they are opening themselves up to information security threats.

Some of the other information security threats for which there are lower levels of preparedness include threats, which may be considered outside the control of IT management. Forces of nature is a good example of a threat, which may not be altogether possible to predict. In addition, addressing quality of service deviations may be perceived as difficult to control. Addressing technological obsolescence is a risk which can be controlled, but which may not be fully safeguarded because of the costs of continuously upgrading technology resources.

IT management faces budgetary constraints. In order to obtain the financial resources needed to upgrade information technology resources, IT management needs to make a business case for the importance of information security, based upon the financial impact of compromised information resources. The importance of making this business case to senior management is one of the relevant findings of this study, because upgrading technological resources is a risk mitigation strategy that is within the jurisdiction of IT management and senior management.

High Impact+Low Probability of Occurrence Risks and Level of Preparedness

In terms of the risks in the high impact+low probability of occurrence quadrant, the levels of preparedness

Table 11. Mean Scores of Impact, Probability, and Preparedness (By Quadrant)

	Impact	*Impact Level*	*Prob*	*Prob Level*	*Quadrant*	*Prep*	*Prep Level*
Legend							
Human Error	4.57	High	4.65	High	4	4.66	2
Intellectual Property Infringement	4.24	High	3.43	Low	3	4.27	2
Acts of Trespass	5.37	High	3.15	Low	3	4.71	2
Acts of Information Sabotage	5.23	High	2.84	Low	3	4.65	2
Acts of Sabotage or Vandalism	5.79	High	2.99	Low	3	4.77	2
Acts of Theft	5.13	High	3.37	Low	3	4.73	2
Software Attacks	5.15	High	4.22	High	4	5.28	3
Forces of Nature	5.23	High	3.63	High	4	4.70	2
Quality of Service Deviation	4.87	High	4.05	High	4	4.65	2
Tech Hardware Failure	4.63	High	4.56	High	4	5.21	3
Tech Software Failure	4.63	High	4.40	High	4	4.98	3
Tech Obsolescence	3.80	High	4.38	High	4	4.63	2

Table 13. High-Impact/Low Probability Risks

Higher-levels of Preparedness	*Lower levels of Preparedness*
	2, Intellectual property 3, Acts of trespass 4, Acts of information extortion 5, Acts of sabotage 6, Acts of Theft

(level 2) were aligned with information security risks (2) Intellectual Property, (3) Acts of Espionage or Trespass, (4) Acts of Information Extortion, (5) Acts of Sabotage or Vandalism, and (6) Acts of Theft. See Table 13.

The lesser levels of preparedness (level 2) aligned with these high impact, low probability risks may be based upon the perception of low probability of occurrence. Even though these risks have high impact, they really are not expected to occur. This is particularly true of acts of espionage or trespass, acts of information extortion, acts of sabotage or vandalism, and acts of theft. If these information security threats do occur, most companies are hesitant to share information about them. Information about the actual extent of these information security breaches may not be publicly available, and this may give a false perception of security against such risks.

Conclusions and Implications for Practice

In summing up, organizations should ask two questions and then develop a risk management strategy. Two of the questions deal with risk assessment are:

1. What is the impact of information security risks?
2. What is the probability of these information security risks occurring?

For the information security risks that are high-impact and high-probability, organizations should implement a risk preparedness strategy, which enables them to safeguard and to mitigate against these risks. In contrast, for low-impact, less-probable risks, information security preparedness may not be as critical.

In this study, the findings showed that for many of the high-impact, high-probability risks, the level of preparedness was aligned with the level of risk. However, in the instances of several risks: 1, Human Error, 8, Forces of Nature, 9, Quality of Service Deviations, 12, Technological Obsolescence, information security preparedness was not aligned with the level of perceived risk. It is these issues, which should be addressed. The issue of human error (e.g., employee mistakes) is particularly relevant because employees may not be aware that they are exposing themselves and their organizations to information security risks. For example, if an employee opens up an e-mail containing a virus, then the magnitude of one risk (e.g., deliberate software attack) is magnified because of another risk factor (e.g., human error).

This study provides opportunities for further research. The data collected here is based upon the respondents' perception of the impact and probability of each risk factor, and their perception of the level of preparedness to deal with these risks. It would be interesting to determine the exact level and nature of protection measures, which are used to mitigate high impact and high probability risks, and this would be a good follow-up study. An information security audit of individuals' workstations and departmental servers would also provide further information about the level of risk exposure that might be due to human factors.

The two implications of this study for practice are: (1) Managers should assess information security risks on an ongoing basis; and (2) Based upon the risk assessment, managers should develop and implement a risk mitigation strategy to minimize these risks.

Acknowledgments

This is to provide credit to the team of students in my CMIS class, Spring, 2007, who assisted with the data collection effort. These students include: Chris Lowe, Chris Klucker, Chris McCloud, Kenton Frere, Rich Guyton, Brian Keyes, Danny Dike, Justin Greek, Caleb Lutz, Casey Kicielinski, and Scott Munn.

Author Bio

Mary Sumner is Professor of Computer Management and Information Systems and Associate Dean, School of Business, Southern Illinois University Edwardsville. In this role, she organizes business/university partnerships and executive education programs. She has written seven textbooks, including college texts in Management Information Systems and Enterprise Resource Planning, and has published over forty research papers on enterprise resource planning, IT workforce issues, and computer-mediated communications. Her research has appeared in Database, the Journal of Information Technology, Information and Management, the Journal of Computer Information Systems, Information Resource Management Journal, and the Proceedings of the ACM SIG MIS Computer Personnel Research (CPR). She has served as Conference Chair, ACM SIGCPR, 1993 (Washington, D.C.), Conference Co-Chair, ACM SIGMIS CPR, 2007 (St. Louis, MO) and Conference Chair, ISECON, 1985. (San Francisco, CA). She oversees the Technology and Commerce Roundtable, a CIO forum.

References

Atkinson, W. (2005). Integrating Risk Management & Security, *Risk Management, 52(10)*, 32–37.

Cerrullo, V., & Cerullo, M. (2004). Business Continuity Planning: A Comprehensive Approach. *Information Systems Management, 2 (3)*, 70–78.

Cook, I. (2007, Feb. 12). Look Out for the Enemy Within. *Financial Times*, London (UK). 10.

Defense Systems Management College. (2001). *Risk Management Guide for DOD Acquisition.* (4th ed.). Fort Belvoir, VA: Defense Acquistion University Press.

Ernst and Young LLP Global Information Security Survey, 2001, 2002, 2003.

Garretson, C. (2007, Feb. 26). Mobile Devices Expose Networks to Security Threats. *Network World, 24(8)*, 11.

Gordon, L., & Loeb, M. (2004). *2004 CSI/FBI Computer Crime and Security Survey.* Computer Security Institute.

Hagg, A. (2002). Benchmark Report: BCP in 2002. *Contingency Planning and Management, 7(5).*

Herold, R. (2006). Addressing Privacy Issues During Disaster Recovery. *Information Systems Security, 14(6)*, 16–23.

Keller, S., Powell, A., Horstmann, B., Predmore, C., and Crawford, M. (2005). Information Security Threats and Practices in Small Business. *Information Systems Management*, *22(2)*, 7–19.

Peiro, A., Cook, P., & Beydoun, H. (2005). *Small Business Information Security Readiness.* Small Business Technology Institute, 1–16.

Pinto, C., Arora, A., Hall, D., & Schmitz, E. (2006). "Challenges to Sustainable Risk Management: Case Example in Information Network Security." *Engineering Management Journal*, *18(1)*, 17–24.

Potter, B., (2006). Wireless Hotspots: Petri Dish of Wireless Security. *Communications of the ACM*, *49(6)*, 51–56.

Roberts, G. K. (2005). Security Breaches, Privacy Intrusions, and Reporting of Computer Crimes, *Journal of Information Privacy & Security, 1(4)*, 22–32.

Ryan, S. D., & Bordoloi, B. (1997). Evaluating security threats in mainframe and client/server environments. *Information & Management*, *32*, 137–146.

Sinnett, W. M., & and Boltin, G. (2006). IT Security, Investment Top CFO Concerns. *Financial Executive, 22(5)*, 42–45.

Stoneburner, G. (2006). Toward a Unified Security/Safety Model. *IEEE Computer*, *39(8)*, 96–97.

Wade, J. (2004). The Weak Link in IT Security. Risk Management, *51(7)*, 32–37.

Waxer, C. (2007, April 12). The Top 5 Internal Security Threats. *Itsecurity.Com*. Retrieved September 9, 2008 from http://www.itsecurity.com/features/the-top-5-internal-security-threats-041207/

Whitman, M. E. (2003). Enemy at the Gate: Threats to Information Security. *Communications of the ACM, 46(8)*, 91.

Wilson, T. (2007, Mar. 9) "Small Businesses: Overconfident on Security." Dark Reading. Retrieved September 9, 2008 from <http://www.darkreading.com/document.asp?doc_id=119107>/