Behaviour & Information Technology
Vol. 29, No. 3, May–June 2010, 221–232

Taylor & Francis
Taylor & Francis Group

Perception of information security

Ding-Long Huang[a]*, Pei-Luen Patrick Rau[a] and Gavriel Salvendy[a,b]

[a]*Department of Industrial Engineering, Tsinghua University, Beijing, China;* [b]*School of Industrial Engineering, Purdue University, West Lafayette, IN, USA*

(*Received April 2007; final version received September 2007*)

The objective of this study was to investigate people's perception of information security and to unveil the factors that influence people's perception of different threats to information security. In the survey study, 602 respondents were asked to evaluate one of 21 common threats to information security with regard to its rank related to each of the 20 threat-related features. An exploratory factor analysis was then conducted, and a six-factor structure was derived, which includes factors of Knowledge, Impact, Severity, Controllability, Possibility and Awareness. Using this factor structure, the characteristics of the five most dangerous threats (hackers, worms, viruses, Trojan horses and backdoor programs) and the five least dangerous threats (spam, piratical software, operation accidents, users' online behaviour being recorded and deviation in quality of service) were discussed and compared. The relationships between the factors and the perceived overall danger of threats were found and then tested by multiple regression analyses. Significant effects were also found in people's perception of information security related to computer experience and types of loss.

Keywords: perception; information security; survey study; factor analysis

1. Objective and significance

Information security (InfoSec) is of great concern to computer and Internet users, who are subject to a variety of threats to information security. Every day there are millions of security incidents due to viruses, hackers, spam, spyware, zombie networks and many other threats to information security (Berinato 2005). These incidents have serious effects on the economy and society (UNCTAD 2005), by bringing about infringements of human rights, financial damage to corporations and the failure of the entire information system. Moreover, these threats to information security can influence IT users' perception and behaviour.

Information security involves both technology and people, and it is becoming increasingly evident that 'the human factor is the Achilles heel of information security' (Gonzalez and Sawicka 2002). Numerous sophisticated security methods have been developed, but information security is deteriorating (Gorden *et al.* 2006, Turner *et al.* 2006). No matter how well designed, security methods rely on individuals to implement and use them. These methods may not accomplish their intended objectives if they are not used properly (Schultz *et al.* 2001). Moreover, many people hesitate or refuse to adopt IT appliances because of worries about security problems (CNNIC 2006), and whether people are willing to adopt an IT appliance depends not only on its 'real security level', but also on its 'perceived security'.

It has been realised that information security is not just a technology problem (Hassel and Wiedenbeck 2004), and in recent years much research has been carried out on human factors in information security. However, little research has been conducted to study people's perception of information security. Perception is a major part of human intelligence and a key component to understand human behaviour (Salvendy 1997). It is the mechanism with which a person evaluates external inputs, which, in turn, determines the behavioural response (Cooper 2003). IT users respond to different kinds of threats according to their perceptions of information security. Overestimates of risk can keep IT applications from being adopted (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, people might refuse to use e-banking because of unnecessary worries about security problems. On the other hand, underestimation of risk can wrongly encourage people to engage in insecure practices (Musekura and Ekh 2004, Stewart 2004, Thomson and von Solms 2005, Chai *et al.* 2006, Gorden *et al.* 2006, Turner *et al.*

*Corresponding author. Email: hdl99@mails.tsinghua.edu.cn

ISSN 0144-929X print/ISSN 1362-3001 online

DOI: 10.1080/01449290701679361
http://www.informaworld.com

2006), for example, people might set simple and weak passwords for their information system because they think the risk of their system being attacked is low. Therefore, what people perceive, why they perceive it that way, and how they will subsequently behave is a matter of great import to the study of human factors in information security, which are essential for a better understanding of IT users' attitude and behaviour.

This research seeks to understand how to better model people's perception of information security, what factors can influence people's perception of information security, and how people perceive different kinds of threats to information security.

2. Background literature

2.1. Information security and threats

Nowadays, people seldom question the benefits of using computers and the Internet for communication and doing business. However, the problem of information security is becoming an increasingly important issue. For common computer and Internet users, information security may mean being able to work with computers without being attacked by viruses, being able to conduct on-line business without worrying that their credit card numbers will be stolen, being able to read e-mails without receiving spam, or being able to talk with friends through instant messaging software without worrying that the information will be wiretapped. According to an official definition, information security is the protection of information and the systems and hardware that use, store and transmit that information (NSTISSC 1994). From a technical viewpoint, information security is to protect the availability, accuracy, authenticity, confidentiality, integrity, utility and possession of information (Whitman and Mattford 2004).

There are many kinds of threats to information security. A threat to information security can be defined as anything indicating the possibility of information being attacked, destroyed or modified (Musekura and Ekh 2004). The 2006 Computer Security Institute/Federal Bureau of Investigation (CSI/FBI) survey on computer crime and security (Gorden *et al*. 2006) found that 72% of respondents (primarily corporations and government agencies) had detected computer security incidents within the last 12 months. The top four types of attack were viruses, laptop/mobile theft, insider abuse of net access and unauthorised access to information, which accounted for more than 74% of financial losses. The 2006 Symantec internet security threat report (Turner *et al*. 2006) claimed that 2249 new vulnerabilities were documented during the first half of 2006, 18% higher than the second half of 2005. 157 477 unique phishing messages were detected, an increase of 81%. Spam made up 54% of all monitored mail traffic, up from 50% in the last period.

The number of threats to information security is almost incalculable and is on the increase. To better understand the numerous threats to information security, a model categorising the threats into 12 general categories has been developed (Whitman 2003, Whitman and Mattford 2004). A list of 21 common threats to information security and their categories in terms of this model is shown in Table 1. These threats are very different from each other. However, they all bring risks to the availability, accuracy, authenticity, confidentiality, integrity, utility or possession of information. In this research, these threats are evaluated with some basic items of perception, which are illustrated in the next section.

2.2. Perception of hazards and perception of InfoSec

Perception of hazards has been a focus of interest of researchers for some decades. How do people perceive different hazards (such as nuclear power, motor vehicles and smoking)? What factors can influence people's risk acceptance? Much research has been carried out on risk perception, dating back to Starr's work, which showed that risk acceptance was related

Table 1. Common threats to information security.

Categories	Threats
1. Acts of human error or failure	Operation accidents
2. Compromises to intellectual property	Piratical software
3. Deliberate acts of espionage or trespass	Hacker, password attack, information wiretapping, users' online behaviour being recorded
4. Deliberate acts of information extortion	Data extortion
5. Deliberate acts of sabotage or vandalism	Denial of service (DoS)
6. Deliberate acts of theft	Computer theft, phishing
7. Deliberate software attacks	Viruses, worms, Trojan horses, backdoor programs, zombie PCs, spam
8. Forces of nature	Natural disasters (such as fire, earthquakes, and lightning)
9. Deviations in quality of service	Deviation in quality of service from service providers
10. Technical hardware failures or errors	Hardware failure
11. Technical software failures or errors	Malicious software
12. Technological obsolescence	Software bugs

not only to technical estimates of risk and benefits but also to a subjective dimension such as voluntariness (Starr 1969).

Starr's work gave rise to much interest in the question of how people perceive risks. The psychometric paradigm was developed and became the most influential model in the field of risk analysis (Fischhoff *et al*. 1978, Slovic *et al*. 1980, Slovic 1987). The aim of the psychometric paradigm is to unveil the factors that determine risk perception (Siegrist *et al*. 2005). An important paper published by Fischhoff *et al*. (1978) indicated that people's perception of different hazards can be influenced by certain factors. They compiled nine items from the literature, including voluntariness of risk, immediacy of effect, known to those exposed, known to science, control over risk, newness, chronic-catastrophic, common-dread and severity of consequences. The subjects were asked to rate a number of hazards for each of the items. The resultant Items × Hazards matrix was factor analysed, and a two-factor (labelled as 'technological risk' and 'severity') solution was achieved. A subsequent study (Slovic *et al*. 1980) extended this research, applying it to a broader set of 18 risk-related items, with a three-factor (labelled as 'dread', 'familiarity' and 'number of people exposed') model. Another factor model was then developed, which consisted of two factors: 'dread risk' (defined at its high end by perceived lack of control, dread, catastrophic potential, fatal consequences and the inequitable distribution of risks and benefits) and 'unknown risk' (defined at its high end by hazards judged to be unobservable, unknown, new, and delayed in their manifestation of harm) (Slovic 1987).

Many studies on risk perception utilising the psychometric paradigm were then carried out. More and more items and their influence on risk perception have been investigated. Examples of these items include Familiarity (Wogalter *et al*. 1991), which states simply that the more familiar people are with a situation or product, the less they perceive associated risk; Catastrophic Potential (Holtgrave and Weber 1993), in which people are more concerned about accidents that are grouped in time and space than accidents that are scattered in time and space; Observability (McDaniels *et al*. 1995), meaning people are more concerned about hazards that are not observable; Impact on Children (Covello and Merkhofer 1994), which states that people are more concerned about risks that can affect children; and Dread (Holtgrave and Weber 1993), which means people are more concerned about risks that have dreaded results. According to Covello (Covello 1983, 1992, Covello and Merkhofer 1994), psychological research has identified 47 known items that influence people's perception of risk.

The study of risk perception has been applied in many fields, such as nuclear engineering (Sjoberg and Drottz-Sjoberg 1991, Stainer and Stainer 1995), epidemiology (Setbon *et al*. 2005), automobile safety (Slovic *et al*. 1987) and construction safety (MacDonald 2006). Some studies have also been carried out in the field of information technology. Jackson *et al*. (2005) reviewed the social science literature on the public perception of risk and extended their discussion to perceptions of crime in cyberspace. Vyskoc and Fibikova (2001) conducted a survey about how IT users perceive information security. The results showed that users do not always think in the same way as security specialists do, and they claimed that real security can be achieved only when employees of the organisation collaborate and behave in a secure way. Yenisey *et al*. (2005) investigated users' feelings of security in e-commerce and developed guidelines for perceived security in e-commerce. In this study, the perception of information security was defined as the mechanism with which a person evaluates threats to information security, which, in turn, determines the behavioural response.

3. Method

Though most of the previous research on risk perception did not consider threats to information security (such as hackers and viruses), the items that have been identified to have an influence on the perception of general hazards may also influence people's perception of information security. In this study, we derived 20 items from a review of the literature and investigated their influence on people's perceptions of information security. Table 2 lists these 20 items and their descriptions in the survey.

An interview was then administered to 20 university students (who had abundant computer and Internet experience) with an in-depth, open-ended questionnaire. Their opinions about the possible issues that could influence their perception of information security were elicited. Their answers validated the items list in Table 2. Additionally, another two items that may influence people's perception of information security were found. One was Type of Loss, which means that different types of loss (such as financial loss, personal information being stolen and waste of time) may lead to different perceptions of information security. The other was Experience with Computers; it seemed that experienced computer users worried less about information security compared with users with less computer experience. The influences of these two items on people's perception of information security were also investigated in this research.

A questionnaire was then constructed and a survey was conducted. Each respondent in this survey was asked to evaluate one of the threats listed in Table 1. The threat was selected from Table 1 randomly, and a brief introduction to this threat would be given. The respondents evaluated the threat with regard to (a) its position relative to each of the 20 items listed in Table 2; (b) its perceived overall risk level; and the (c) type of loss it would cause. For the first two types of questions, the seven-point Likert scale anchored with opposing adjective phrases was used. Point one referred to strongly disagree and point seven referred to strongly agree. For the question of 'type of loss the threat will bring about', there were six options (multiple choice): financial loss, exposure of personal information, inconvenience of computer use, waste of time, loss of reputation and loss of data. Demographic information including the respondent's age, gender, education level, occupation, experience with computers and the Internet, knowledge about computers, and the security methods they had adopted were collected.

The target population of this survey was people who had experience using computers and the Internet. The survey was posted on the website of the IT Usability Laboratory of Tsinghua University, China, which could be accessed by all Internet users. The number of respondents participating in the survey study was 646. Among all the cases, 44 of them were found to be invalid because of incomplete or inconsistent responses. So the total sample size used in the data analysis was 602. There were 381 males (63%) and 221 females (37%) ranging in age from 17 to 51 (mean = 24.3, SD = 5.17).

Table 2. Survey-derived items that may influence users' perception of information security.

Items	Description in the survey
1. Familiarity	I am familiar with this threat.
2. Severity of consequences	The consequences of this threat are serious.
3. Voluntariness	I am exposed to the risk of this threat voluntarily.
4. Catastrophic potential	The outcomes of this threat are grouped in time and space (instead of being scattered in time and space).
5. Understanding	I understand this threat.
6. Personal exposure	This threat causes personal harm (instead of public harm).
7. Observability	This threat is observable.
8. Ease of reduction	The effect of this threat can be reduced easily.
9. Preventive control	This threat can be prevented.
10. Control of severity	The severity of the effect of this threat can be controlled.
11. Immediacy of effect	The effects of this threat are apparent immediately.
12. Known to those exposed	The existence of this threat can be known to those exposed to it.
13. Newness	This threat is a new or novel one.
14. Media attention	The media pays much attention to this threat (media such as newspapers, TV and Websites).
15. Accident history	I have never been exposed to this threat.
16. Reversibility	The effect of this threat can be reversed.
17. Duration of impacts	The duration of the impacts of this threat is long.
18. Scope of impacts	The scope of the impacts of this threat is wide.
19. Predictability	This threat can be predicted.
20. Possibility	The possibility that I will be exposed to this threat is large.

4. Results

4.1. Overview

Table 3 lists the mean and standard deviation of the scores for the 20 items arranged from lowest score to the highest score. The Severity of Consequence item had a high mean score of 5.5 (SD = 1.38). This indicated that most respondents considered those threats to information security as having serious consequences. The Personal Exposure item had a low mean score of 2.7 (SD = 1.60), which showed that the respondents considered that those threats not only harm them personally, but also cause public harm.

Table 3. Descriptive statistics of survey responses ($N = 602$).

Items	Mean	SD
Personal exposure	2.7	1.60
Newness	3.1	1.52
Catastrophic potential	3.4	1.55
Voluntariness	3.5	1.61
Understanding	3.6	1.76
Reversibility	3.7	1.44
Immediacy of effect	3.7	1.55
Control of severity	3.9	1.68
Media attention	3.9	1.62
Known to those exposed	3.9	1.62
Familiarity	4.0	1.76
Predictability	4.2	1.45
Duration of impacts	4.4	1.41
Possibility	4.5	1.49
Observability	4.5	1.56
Preventive control	4.6	1.67
Accident history	4.8	1.80
Scope of impacts	5.0	1.36
Ease of reduction	5.1	1.51
Severity of consequence	5.5	1.38

4.2. Factor analysis

To explore the latent structure of the 20 items and identify the factors that can influence people's perception of information security, an exploratory factor analysis was conducted on the raw data. Before performing the factor analysis, the Kaiser – Meyer – Olkin Measure of sampling adequacy (KMO) test was employed to check whether the 20 items were suitable for a factor analysis. The KMO test result (value 0.641) was substantially higher than the acceptable exploratory research norm of 0.5 established by Nunnally (Nunnally 1978). Six factors were extracted using a screen test; all of them evolved with eigenvalues that were greater than 1 and accounted for 51.6 percent of the total variance. The factors were rotated by the EQUAMAX method. The results of factor analysis are shown in Table 4, with the highest entries in each row highlighted in gray.

As shown in Table 4, the results of factor analysis clearly clustered the related items together. Factor 1 contains four items: Familiarity, Understanding, Control of Severity and Newness. These items are related to people's knowledge of the threats to information security. People usually know little about new threats; they also feel unfamiliar with them, and find them hard to understand and their severity hard to control. Therefore this factor was referred to as 'Knowledge'.

Factor 2 includes the Duration of Impacts', Scope of Impacts and Media Attention. These items are related to the impacts of the threats. People are concerned about how long the duration is, how wide the scope is, and how much media attention is paid to the threats. Thus, this factor was designated as 'Impact'.

Factor 3 contains Personal Exposure, Voluntariness and Severity of Consequence. This factor reflects how people perceive the severity of the threats to information security. High scores on this factor were associated with threats that can have serious consequences, cause public harm, and cause people to be exposed to risk involuntarily. It seems appropriate to label this factor as 'Severity'.

Factor 4 includes six items: Preventive Control, Observability, Ease of Reduction, Reversibility, Predictability and Catastrophic Potential. This factor indicates to what extent people can control the threats, whether the threats can be prevented, observed, reversed and predicted, whether their effect can be reduced, and whether their outcomes are scattered in time and space. Thus, factor 4 was labelled as 'Controllability'.

Factor 5 contains the items of Accident History and Possibility. People may perceive a relatively high possibility of being exposed to a threat if they have already been exposed to it in the past. So this factor was named 'Possibility'.

Table 4. Factor analysis of items influencing perception of InfoSec.

Items	Factors						Communality estimates
	1	2	3	4	5	6	
Familiarity	0.719	0.045	0.016	−0.093	0.261	0.108	0.607
Understanding	0.730	0.033	0.004	0.056	−0.173	0.091	0.575
Control of severity	0.546	−0.025	0.305	0.314	−0.027	0.150	0.514
Newness*	0.430	−0.091	−0.349	0.039	0.214	−0.291	0.447
Duration of impacts	−0.031	0.790	−0.105	−0.104	−0.023	0.002	0.647
Scope of impacts	0.016	0.794	−0.215	0.053	0.132	0.046	0.700
Media attention	0.043	0.440	0.243	0.096	0.060	−0.073	0.273
Personal exposure	−0.083	−0.008	0.591	−0.178	0.085	0.232	0.449
Voluntariness	0.181	0.052	0.608	0.137	−0.054	−0.092	0.436
Severity of consequence*	0.008	−0.152	0.755	0.04	−0.093	0.048	0.606
Preventive control	0.149	−0.167	−0.176	0.546	−0.278	−0.185	0.491
Observability	0.088	0.018	0.005	0.510	0.123	0.441	0.478
Ease of reduction	0.157	−0.001	0.001	0.629	0.059	0.103	0.435
Reversibility	−0.128	0.103	0.265	0.485	−0.172	0.073	0.367
Predictability	0.037	0.355	0.104	0.548	0.085	−0.008	0.446
Catastrophic potential*	−0.005	−0.144	−0.166	0.422	0.097	−0.404	0.398
Accident history	0.088	−0.089	−0.094	−0.034	0.816	0.023	0.692
Possibility	−0.038	0.251	0.032	0.061	0.724	−0.072	0.598
Immediacy of effect	−0.012	−0.086	−0.036	−0.014	−0.076	0.787	0.634
Known to Those Exposed	0.243	−0.003	0.093	0.140	0.044	0.651	0.514
Variance explained by each factor	1.716	1.750	1.781	1.878	1.525	1.656	10.307
% Variance explained by each factor	8.6	8.7	8.9	9.4	7.6	8.3	51.6

*Scores of the items marked with asterisks have been reversed.
Highlighted in gray are the highest entries in each row.

Factor 6 includes two items: Immediacy of Effect and Known to Those Exposed. These items are related to the awareness of the threats. Those threats whose effects are shown immediately are usually more likely to be known to those exposed to them. Therefore, this factor was labelled as 'Awareness'.

The reliabilities of these factors were assessed by Cronbach's alpha coefficient and the results showed that they were almost all over 0.5 and satisfied the exploratory research norm set by Nunnally (Nunnally 1978), except one factor, 'Severity', whose Cronbach's alpha value was 0.484. The Severity factor includes three items: Personal Exposure, Voluntariness and Severity of Consequence. Looking into the raw data, a trend could be found that those threats perceived as causing public harm were usually also perceived as causing people to be exposed to threats involuntarily and having serious consequences. However, the situation is special for the threat of 'computer theft', which was perceived as causing personal harm, but still causing people to be exposed to threats involuntarily and having serious consequences. The special situation of 'computer theft' is understandable considering that it is the only physical threat within these 21 threats. So the Cronbach's alpha coefficient for the Severity factor was re-computed using the data of the other 20 threats, and the results were well over the 0.5 exploratory research norm set by Nunnally (Nunnally 1978).

It should be noted that although orthogonal rotation (Equamax rotation) was used in the factor analysis, these six factors are more or less interrelated. Some items had relatively high loadings on more than one factor. For example, the items of Observability and Catastrophic Potential had the highest loading on factor 4 (controllability), yet their loading (absolute value) on factor 6 (awareness) was also above 0.4. This indicated that those threats that could be observed and were grouped in time and space were also easier to detect.

4.3. *Characteristics of threats*

The mean scores of items belonging to each of the six factors were computed (referred to as the 'mean factor score' in the rest of this paper). Comparisons of the mean factor scores and the perceived overall danger among the 21 threats to information security were conducted, using analysis of variance (ANOVA). The results are shown in Table 5.

Significant differences were found in the mean scores for the factors Knowledge, Impact, Severity, Possibility and Awareness, indicating that these five

Table 5. Comparisons of mean factor scores and perceived overall danger among threats.

Number	Threats	*N*	Factors*						Overall danger
			1	2	3	4	5	6	
1	Backdoor programs	26	3.82	4.59	5.18	4.13	5.15	3.23	6.04
2	Trojan horses	29	4.28	4.23	5.29	4.54	5.36	4.03	5.83
3	Hackers	34	4.14	4.86	5.47	4.37	4.43	3.56	5.71
4	Worms	31	4.02	4.83	5.56	4.56	4.56	3.90	5.68
5	Viruses	28	4.19	4.55	5.14	4.53	5.57	4.23	5.68
6	Denial-of-service (DoS)	31	3.98	4.25	5.29	4.42	4.29	4.19	5.65
7	Phishing	25	4.17	4.28	5.15	4.71	4.40	3.60	5.56
8	Computer theft	28	4.47	4.46	5.11	4.20	3.68	4.25	5.54
9	Password attack	28	4.32	3.87	5.30	4.51	4.23	2.77	5.50
10	Information wiretapping	26	4.01	4.82	4.86	4.54	4.19	2.79	5.50
11	Zombie PCs	29	3.56	4.34	5.56	4.46	4.22	3.95	5.48
12	Hardware failure	31	3.89	4.38	4.76	4.44	4.61	4.39	5.48
13	Natural disasters (such as fires, earthquakes, and lightning)	28	4.42	4.60	5.48	4.32	4.25	4.39	5.43
14	Faulty software	25	4.42	4.55	5.03	4.48	5.28	4.16	5.40
15	Software bugs	31	3.98	4.23	5.27	4.30	5.21	3.42	5.39
16	Data extortion	30	3.23	4.34	5.04	4.70	3.55	3.50	5.33
17	Users' online behaviour being recorded	23	4.08	4.42	4.28	4.25	5.02	3.04	5.26
18	Operation accidents	31	4.37	3.92	4.75	4.63	4.44	3.97	5.26
19	Deviation in quality of service from service providers	30	4.10	4.39	5.11	4.33	4.83	4.4	5.20
20	Piratical software	26	4.32	4.78	4.31	4.48	4.69	3.50	5.00
21	Spam	32	4.70	4.50	4.84	4.69	5.36	4.45	4.91
F			2.939	2.011	3.190	1.095	5.600	5.386	1.704
p			<0.001	0.006	<0.001	0.350	<0.001	<0.001	0.029

*Factor 1, knowledge; factor 2, impact; factor 3, severity; factor 4, controllability; factor 5, possibility; factor 6, awareness.

factors could be the characteristics that distinguish different threats to information security. There was no significant difference found in the mean scores of the Controllability factor. It seemed that the 21 threats were all perceived as slightly controllable (having mean scores within 4.1 – 4.8).

Significant differences were also found in perceived overall danger related to different threats. The five types of threats with the highest scores of perceived overall danger were backdoor programs, Trojan horses, hackers, worms and viruses. And the five types of threats with the lowest scores of perceived overall danger were spam, piratical software, deviation in quality of service from service providers, operation accidents and users' online behaviour being recorded.

The characteristics of these five most dangerous threats and five least dangerous threats and the reasons why they were perceived as dangerous to different extents could be explained, using the six-factor structure achieved from the factor analysis.

Characteristics of the five most dangerous threats: hackers and worms had similar characteristics. They were both located at the high end of Impact and Severity (as shown in Figures 1a and 1b), indicating that they were perceived as having conspicuous impacts and bringing serious consequences. Viruses and Trojan horses were similar and were both located at the high end of Possibility (as shown in Figures 1c and 1d), indicating that people perceived a high possibility of encountering them. Backdoor programs was located at the high end of Possibility and low end of Awareness (as shown in Figure 1e), and also had a low score for Controllability (though no significant difference was detected), indicating that people not only perceived a high possibility of encountering them, but also felt that this threat was hard to detect and control. This might be the reason that it was perceived as the most dangerous threat.

Characteristics of the five least dangerous threats: Compared with viruses and Trojan horses, spam was also high at the end of Possibility. However, it had high scores of Awareness and Knowledge (as shown in Figure 2a), indicating that people thought that they knew spam quite well and they could easily detect it, which might be why they perceived spam as the least dangerous threat. Piratical software and users' online behaviours being recorded both had low Severity scores (as shown in Figures 2b and 2c). People thought they would not have serious consequences. Users' online behaviour being recorded also had an extremely low Awareness score. People usually did not know whether their online behaviour had been recorded. In contrast, deviation in quality of service from service providers had a high Awareness score (as shown in Figure 2d), indicating that it could easily be detected by users. Operation accidents was located at the low end of Impact (as shown in Figure 2e), indicating that people did not perceive the impact of this threat to be too severe.

Through this investigation of the characteristics of the most dangerous and least dangerous threats, some relationships between the factors and the perceived overall danger could be seen. These relationships were tested by multiple regression, as described in the next section.

4.4. Multiple regression analysis

To investigate how the perceived overall danger of the threats to information security can be predicted by the items and factors, multiple regression analysis was conducted. Using the 'overall danger level' as the dependent variable, and the 20 threat-related items as the independent variables, a stepwise multiple regression analysis was performed to select the significant independent variables. As a result, seven items were selected, which together accounted for 18.3% of the respondents' overall perceived danger. Table 6 shows the seven selected items, which included: Severity of Consequences, Scope of Impacts, Accident History, Voluntariness, Duration of Impacts, Understanding, and Possibility.

Similarly, using the 'overall danger level' as the dependent variable, and the six factors extracted from factor analysis as the independent variables (the factor scores for each case were computed with a factor loading matrix), a stepwise multiple regression analysis was performed to investigate which factors best predict the overall perceived danger of threats to information security. The results are shown in Table 7. The factors Severity, Impact, Possibility and Knowledge were found to have a significant effect, and together they accounted for 17.7% of the respondents' overall perceived danger.

When the results from the two multiple regression analyses are looked at together, it can be seen more clearly that these four significant factors are indeed important for predicting the overall perceived danger of different threats, because most of their contributing items were also selected as significant.

The results indicated that the perceived overall danger of different threats to information security was positively related to the factors of Severity, Impact, and Possibility. This could also be illustrated by threats of hackers (Figure 1a), worms (Figure 1b), viruses (Figure 1c), Trojan horses (Figure 1d), backdoor programs (Figure 1e), piratical software (Figure 1b), users' online behaviour being recorded (Figure 1c) and operation accidents (Figure 1e).

The results also indicated that the perceived overall danger of different threats to information security was negatively related to the factor of Knowledge, which

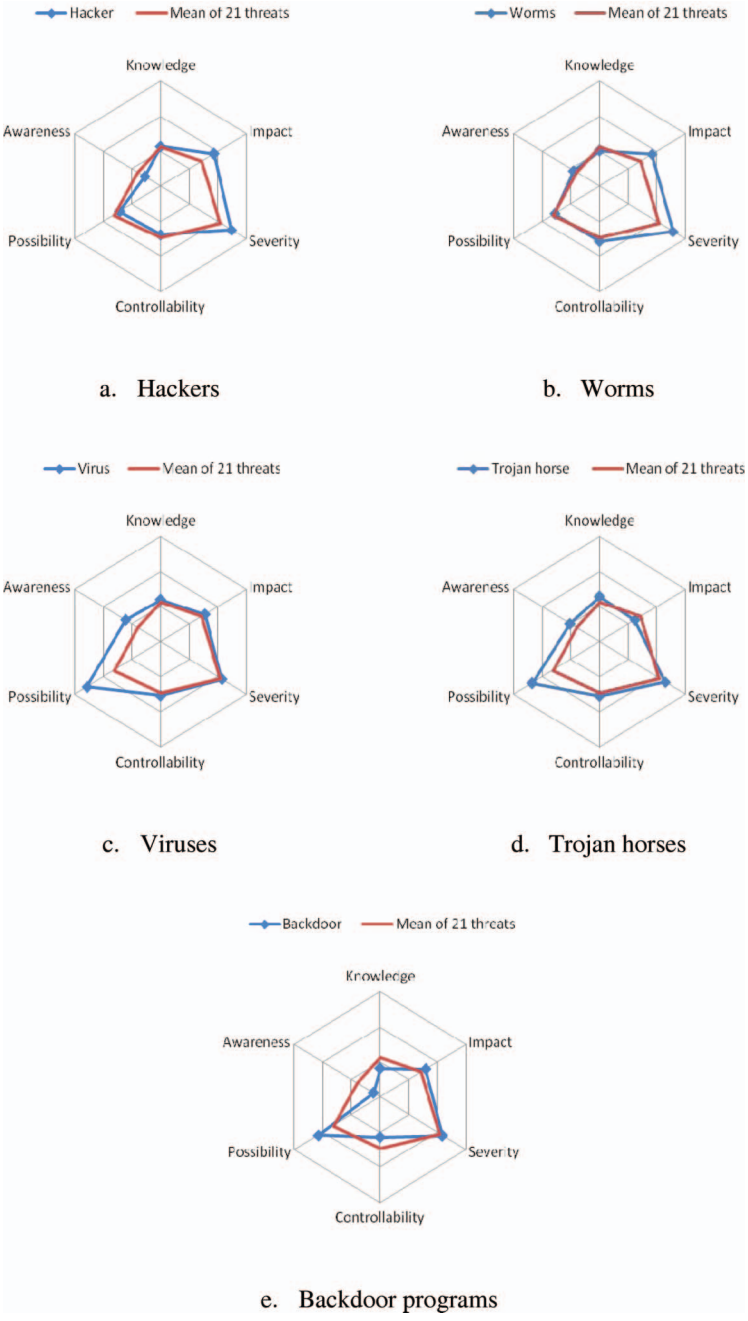

Figure 1. Characteristics of the five most dangerous threats. (a) Hackers; (b) worms; (c) viruses; (d) Trojan horses; (e) backdoor programs.

could be illustrated by the threats of spam (Figure 1a) and operation accidents (Figure 1e).

4.5. *Effect of computer experience*

Computer experience is a people-related variable that may influence people's perception. The effects of a user's computer experience on their perception of InfoSec were tested. Using respondents' frequency of computer use as an independent variable, and their scores for each item and factor as dependent variables, an analysis of variance (ANOVA) was conducted. The results are shown in Table 8. Significant differences were found in the Knowledge factor and in the Newness and Personal Exposure items. Marginal significant differences were found in the Understanding and Ease of Reduction items. Naturally, experienced computer users knew more about threats to InfoSec, perceived those threats as not so novel, had better understanding of those threats and felt it would be

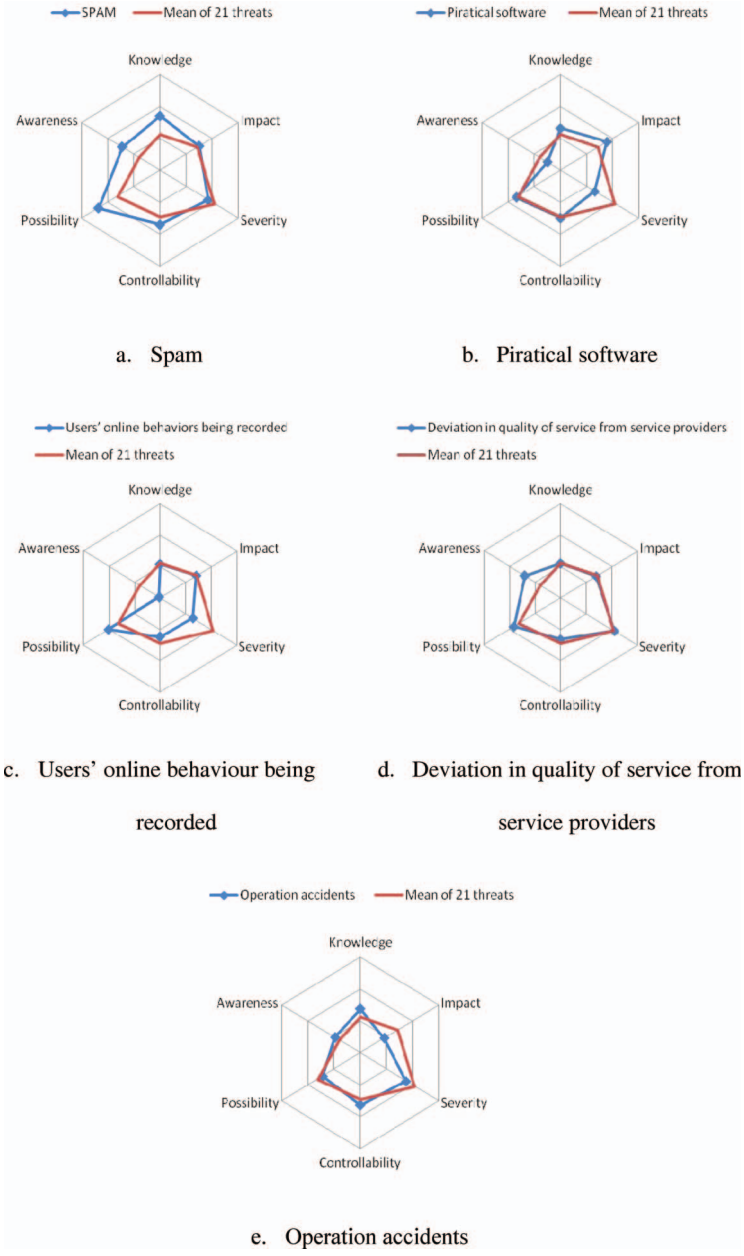

Figure 2. Characteristics of the five least dangerous threats. (a) Spam; (b) piratical software; (c) users' online behaviour being recorded; (d) deviation in quality of service from service providers; (e) operation accidents.

Table 6. Prediction of overall perceived danger: Stepwise selection of items.

Items	Coefficients	F	p
Severity of consequence	0.232	75.512	<0.001
Scope of impacts	0.134	51.085	<0.001
Accident history	0.104	38.331	<0.001
Voluntariness	-0.106	31.081	<0.001
Duration of impacts	0.090	26.280	<0.001
Understanding	-0.082	22.815	<0.001
Possibility	0.081	20.243	<0.001

easier to reduce the effects of those threats. It was also interesting to find that experienced computer users perceived the threats as harmful to the public, while users with less experience perceived the threats as causing personal harm.

4.6. *Effect of loss type*

Different threats to information security can bring different types of loss, which may be perceived differently by different people. The effects of loss type

on people's perception of information security were tested, using the types of loss that respondents selected for each threat as independent variables, and the overall danger as dependent variables. There were six options (multiple choice) for each threat: financial loss, exposure of personal information, inconvenience of computer use, waste of time, loss of reputation and loss of data. Therefore there were six independent variables, each containing two levels (yes or no). The results of six-way ANOVA showed that significant differences were found related to financial loss ($F = 8.663$, $p = 0.003$) and inconvenience of computer use ($F = 4.721$, $p = 0.030$), indicating that people were very concerned about whether the threats could bring financial loss, and whether the threats could make it inconvenient to use computers. Marginal significant differences were found related to waste of time ($F = 3.196$, $p = 0.074$), indicating a trend that people might also care about whether dealing with the threats would waste their time. It was somewhat surprising to find that the respondents did not care about exposure of personal information ($F < 0.001$, $p = 0.992$). Considering that all the respondents in this research were Chinese users, this might be due to cultural influences. It would be an interesting topic to investigate whether Chinese people care less about personal information privacy compared with users from western countries.

4.7. General discussion

The objectives of this study were to investigate the factors that can influence perception of information security and provide a better understanding of people's perception of information security. From the results of this study, it was shown that people's perception of information security can be identified and quantified with certain factors. The essence of the results of this study can be summarised as follows:

- Through a survey study and an exploratory factor analysis, a six-factor structure characterising people's perception of different threats to information security was developed. This model contains factors of knowledge (K), impact (I), severity (S), controllability (C), awareness (A) and possibility (P). The 'KISCAP' model and their components, together with the explanations of their low and high ends, are shown in Table 9.
- The results of ANOVA indicated that the 21 different threats could be well distinguished with the six-factor structure. The characteristics of the five threats perceived as most dangerous and the five threats perceived as least dangerous were discussed and compared with the six-factor structure.
- The relationships between these factors and the perceived overall danger of threats were found and then tested by multiple regression analysis. The results indicated that the factors of Knowledge, Impact, Severity and Possibility had a significant effect on the perceived overall danger of the threats.
- Significant differences in perception of information security were found to be related to the user's computer experience.
- Significant differences in perception of information security were related to the type of loss that the threats could bring.
- It was somewhat surprising to find that the respondents did not care much about personal information privacy. Considering that all the respondents in this research were Chinese users, this might be due to the effect of cultural influences.

Caution needs to be exercised in applying the findings since this study was limited in several aspects.

Table 7. Prediction of overall perceived danger: Stepwise selection of factors.

Factors	Coefficients	F	p
Severity	0.269	46.764	<0.001
Impact	0.238	44.394	<0.001
Possibility	0.210	41.735	<0.001
Knowledge	-0.084	32.790	<0.001

Table 8. Comparison of computer use frequency.

	Every day		Several times per week		Several times per month			
Variables	Mean	SD	Mean	SD	Mean	SD	F	p
Items								
Understanding	3.7	1.77	3.3	1.76	2.2	1.30	2.378	0.069
Newness	3.0	1.50	3.6	1.59	3.6	1.14	3.054	0.028
Personal exposure	2.7	1.56	3.0	1.90	4.2	1.48	2.857	0.036
Ease of reduction	5.1	1.48	4.8	1.75	4.0	1.23	2.172	0.090
Factor								
Knowledge	4.2	1.06	3.8	1.16	3.2	0.88	3.648	0.013

Table 9. Summary of the KISCAP model: Factors and their components.

Factor and its components	Low end	High end
Factor 1: Knowledge		
Familiarity	Not familiar	Familiar
Understanding	Do not understand	Understand
Control of severity	Can not control the severity	Can control the severity
Newness*	New threat	Old threat
Factor 2: Impact		
Duration of impacts	Short duration of impacts	Long duration of impacts
Scope of impacts	Small scope of impacts	Large scope of impacts
Media attention	Little media attention paid	Much media attention paid
Factor 3: Severity		
Personal exposure*	Causing personal harm	Causing public harm
Voluntariness*	Voluntary	Not voluntary
Severity of consequences*	Consequences not serious	Consequences serious
Factor 4: Controllability		
Preventive control	Not preventable	Preventable
Observability	Not observable	Observable
Ease of reduction	Not easily reduced	Easily reduced
Reversibility	Not reversible	Reversible
Predictability	Not predictable	Predictable
Catastrophic potential*	Grouped in time and space	Scattered in time and space
Factor 5: Awareness		
Immediacy of effect	Effect shown after a long time	Effect shown immediately
Known to those exposed	Unknown to those exposed	Known to those exposed
Factor 6: Possibility		
Accident history	Never	Often
Possibility	Low	High

*Scores of the items marked with asterisks have been reversed.

People-related features, such as cultural style (Douglas and Wildavsky 1982), personality (Sjoberg 2003) and risk sensitivity (Sjoberg 2000) were not investigated in this study. Further, there are numerous threats to information security, and the number is growing every day (Turner *et al.* 2006). This study investigated twenty-one common threats. More findings may be achieved if more threats are taken into account.

5. Conclusions

Given the fact that information security has become a serious problem and a great concern for computer users, it is imperative to study people's perception of information security. This is an exploratory study seeking a better understanding of people's perception of information security. A six-factor structure was developed, which can be used to model people's perception of information security, characterise different threats to information security, and predict the perceived overall danger of different threats to information security. This factor structure can be applied in the development and evaluation of security methods, guidelines for adjusting perceived dangers of IT appliances, and policies to encourage computer users to engage in secure behaviours.

Further research could benefit from focusing on the relationship between people's perception of information security and their attitudes toward IT appliances and security methods.

References

Berinato, S., 2005. The Global State of Information Security 2005. Available online at: http://www.csoonline.com/read/100105/survey.html) (accessed 16 April 2006).

Chai, S., Bagchi-Sen, S., Morrell, C., Rao, H.R., and Upadhyaya, S., 2006. Role of perceived importance of information security: an exploratory study of middle school children's information security behavior. *In*: *Informing Science and Information Technology Conference Pro*. 2006, Greater Manchester, England.

China Internet Network Information Center, 2006. The statistics report of the development of Internet in China. Available online at: http://www.cnnic.net.cn/index/0E/00/11/index.htm (accessed 17 April 2006).

Cooper, D., 2003. Psychology, risk & safety: understanding how personality & perception can influence risk taking. *Professional Safety*, 48, 39–46.

Covello, V.T., 1983. The perception of technological risks: a literature review. *Technological Forecasting Social Change*, 23, 285–297.

Covello, V.T., 1992. Risk communication: an emerging area of health communication research. *In*: S. Deetz, ed. *Communication Yearbook*. 15th ed., pp. 359–373 (Beverly Hills: Sage).

Covello, V.T. and Merkhofer, M.W., 1994. *Risk assessment methods*. New York: Plenum.

Douglas, M. and Wildavsky, A., 1982. *Risk and culture*. Berkeley: University of California Press.

Featherman, M.S. and Pavlou, P.A., 2003. Predicting e-services adoption: a perceived risk facets perspective. *International Journal of Human-Computer Studies*, 59, 451–474.

Fischhoff, B., Slovic, P., Lichtenstein, S., Read, S., and Cambs, B., 1978. How safe is safe enough? A psychometric study of attitudes towards technological risks and benefits. *Policy Sciences*, 9, 127–152.

Gonzalez, J.J. and Sawicka, A., 2002. A framework for human factors in information security. *In*: *Proceedings of the 2002 WSEAS International Conference on Information Security (ICIS'02)*, Rio de Janeiro.

Gorden, L.A., Loeb, M.P., Lucyshyn, W., and Richardson, R., 2006. 2006 CSI/FBI computer crime and security survey. Available online at: http://www.gocsi.com (accessed 9 January 2007).

Hassel, L. and Wiedenbeck, S., 2004. *Human Factors and Information Security*. DIMACS Workshop on Usable Privacy and Security Software, 7–8 July 2004, DIMACS Centre, CORE Building, Rutges University, Piscataway, NJ.

Holtgrave, D.R. and Weber, E.U., 1993. Dimensions of risk perception for financial and health risks. *Risk Analysis*, 13, 553–558.

Jackson, J., Allum, N., and Gaskell, G., 2005. Perceptions of risk in cyberspace. *In*: R. Mansell and B.S. Collins, eds. *Trust and Crime in Information Societies*. Cheltenham: Edward Elgar. Available online at http://www/lse.ac.uk/collections/methodologyInstitute/pdf/JonJackson/perceptions%2007%20risk%20in%20cyberspace.pdf.

Jih, W.-J., Wong, S.-Y., and Chang, T.-B., 2005. Effects of perceived risks on adoption of Internet banking services: an empirical investigation in Taiwan. *International Journal of e-Business Research*, 1, 70–88.

Lim, N., 2003. Consumers' perceived risk: sources versus consequences. *Electronic Commerce Research and Applications*, 2, 216–228.

MacDonald, G., 2006. Risk perception and construction safety. *Proceedings of the Institution of Civil Engineers: Civil Engineering*, 159, 51–56.

McDaniels, T., Axelrod, L.J., and Slovic, P., 1995. Characterizing perception of ecological risk. *Risk Analysis*, 15, 575.

Musekura, J.B. and Ekh, R., 2004. Information security issues – difference between perception and practice in organizations. Available online at: http://www.oru.se/templates/oruExtNormal____19402.aspx (accessed 6 January 2007). Department of Business, Economics, Statistics and Informatics, Orebro University, Sweden.

NSTISSC, 1994. National Training Standard for Information Systems Security (Infosec) Professionals. National Security Telecommunications and Information Systems Security Committee.

Nunnally, J.C., 1978. *Psychometric theory*. New York: McGraw-Hill.

Pikkarainen, T., Pikkarainen, K., Karjaluoto, H., and Pahnila, S., 2004. Consumer acceptance of online banking: an extension of the technology acceptance model. *Internet Research*, 14, 224–235.

Salvendy, G., 1997. *Handbook of human factors and ergonomics*. New York: Wiley-Interscience.

Schultz, E.E., Proctor, R.W., Lien, M.C., and Salvendy, G., 2001. Usability and security: an appraisal of usability issues in information security methods. *Computers and Security*, 20, 620.

Setbon, M., Raude, J., Fischler, C., and Flahault, A., 2005. Risk perception of the "mad cow disease" in France: determinants and consequences. *Risk Analysis*, 25, 813–826.

Siegrist, M., Keller, C., and Kiers, H.A.L., 2005. A new look at the psychometric paradigm of perception of hazards. *Risk Analysis*, 25, 211–222.

Sjoberg, L., 2000. Factors in risk perception. *Risk Analysis*, 20, 1–11.

Sjoberg, L., 2003. Distal factors in risk perception. *Journal of Risk Research*, 6, 187.

Sjoberg, L. and Drottz-Sjoberg, B.-M., 1991. Knowledge and risk perception among nuclear power plant employees. *Risk Analysis*, 11, 607.

Slovic, P., 1987. Perception of risk. *Science*, 236, 280–285.

Slovic, P., Fischhoff, B., and Lichtenstein, S., 1980. Facts and fears – understanding risk. *Societal Risk Assessment – How Safe is Safe Enough?*. New York: Plenum, 181–218. R.C. Schwing and W.A. Albers (Eds.).

Stainer, A. and Stainer, L., 1995. Young people's risk perception of nuclear power – a European viewpoint. *International Journal of Global Energy Issues*, 7, 261–270.

Starr, C., 1969. Social benefit versus technological risk. *Science*, 165, 1232–1238.

Stewart, A., 2004. On risk: perception and direction. *Computers and Security*, 23, 362–370.

Suh, B. and Han, I., 2003. The impact of customer trust and perception of security control on the acceptance of electronic commerce. *International Journal of Electronic Commerce*, 7, 135–161.

Thomson, K. and von Solms, R., 2005. Information security obedience: a definition. *Computers & Security*, 24, 69–75.

Turner, D., Entwisle, S., Fossi, M., Blackbird, J., McKinney, D., Conneff, T., and Whitehouse, O., 2006. Symantec Internet security threat report – trends for January 06 to June 06. Available online at: http://www.symantec.com (17 January 2007).

UNCTAD, 2005. Information economy report (United Nations Conference on Trade and Development). Available online at: http://www.unctad.org (accessed 17 April 2006).

Vyskoc, J. and Fibikova, L., 2001. IT users' perception of information security. *In*: *2nd Working Conference on Security and Control of Information Technology in Security*, Bratislava, Bratislava: Comenius University, 107.

Whitman, M.E., 2003. Enemy at the gate: threats to information security. *Communications of the ACM*, 46, 91–95.

Whitman, M.E. and Mattford, H.J., 2004. *Principles of information security*. Boston, MA: Thomson Learning.

Wogalter, M.S., Brelsford, J.W., Desaulniers, D.R., and Laughery, K.R., 1991. Consumer product warnings. The role of hazard perception. *Journal of Safety Research*, 22, 71.

Yang, K.C.C., 2005. Exploring factors affecting the adoption of mobile commerce in Singapore. *Telematics and Informatics*, 22, 257–277.

Yenisey, M.M., Ozok, A.A., and Salvendy, G., 2005. Perceived security determinants in e-commerce among Turkish university students. *Behaviour & Information Technology*, 24, 259–274.