

Perceptions of End Users on the Requirements in Personal Firewall Software: An Exploratory Study

SUNIL HAZARI, University of West Georgia, USA

Citation:

Hazari, S. I. (2005). Perceptions of end-users on the requirements in personal firewall software: An exploratory study, *Journal of Organizational and End User Computing*, 17(3), 47-65.

ABSTRACT

Information security is usually considered a technical discipline with much attention being focused on topics such as encryption, hacking, break-ins, and credit card theft. Security products such as anti-virus programs and personal firewall software are now available for end-users to install on their computers to protect against threats endemic to networked computers. The behavioral aspects related to maintaining enterprise security have received little attention from researchers and practitioners. Using Q-sort analysis, this study used students as end users in a graduate business management security course to investigate issues affecting selection of personal firewall software in organizations. Based on the Q-sort analysis of end users in relation to seven variables identified from review of the information security literature, three distinct group characteristics emerged. Similarities and differences between groups are investigated and implications of these results to IT managers, vendors of security software and researchers in information security area are discussed.

Keywords: Information security, personal firewalls, software feature requirements, Q-Sort analysis.

INTRODUCTION

Information must be readily available in organizations for making decisions to support the organizational mission. Murphy, Boren, and Schlarman (2000) state that due to increased connectivity and the urgency to exchange information and data among partners, suppliers, and customers on a real time basis, the need to protect and secure computer resources is greater than ever. As a result, this has created the possibility of exposing sensitive corporate information to competitors as well as hackers who can now access organizational computer resources from remote sites. The potential loss of such information to an organization goes beyond financial losses and includes the possibility of corrupted data, denial of services to suppliers, business partners and customers, loss of customer confidence, and lost sales. Security in business processes (i.e. maintaining proper authentication, authorization, non-repudiation and privacy) is critical to successful e-business operations. Enabling business functions over the Internet has been recognized as a major component for the success of businesses and by mitigating risks in a cost-effective manner, security is now being viewed as a component of business operations (Deise, Nowikow, King, and Wright, 2000). Decisions about information systems made by managers are vital to the success, and even survival of a firm (Enns, Huff, and Golden, 2003).

Despite increased security threats, organizations have traditionally allocated very little of the total IT budget to information security. Forrester Research estimates that in Fortune 500 companies, the average amount of money as a percent of revenue that is spent on IT security is .0025 percent or slightly less than what they spend on coffee (Clarke, 2002). Organizations must evaluate and prioritize the optimum mix of products and services to be deployed for protecting confidentiality (maintaining privacy of information), integrity (maintaining information is not altered in transit), and availability (maintaining access to information and resources) of corporate assets. The decision to deploy certain technology is based on variables such as the organizational business model, level of risk, vulnerability, cost, and return on investment (Highland, 1993).

There are several ways in which information can be protected. One method to safeguard information is by using controls. The concept of controls can be applied to financial auditing as well as technical computer security. General controls include personnel, physical and organizational controls as well as technical security services and mechanisms (Summers, 1997). Computer security controls can be hardware or software based and may include biometric devices, anti-virus software, smart cards, firewalls, and intrusion detection systems that can be used to build the enterprise security infrastructure. Additionally, these controls may be preventive, detective, or corrective. This paper will focus on one such computer security control – Personal Firewalls. Firewalls intercept traffic and make routing and redirection decisions based on policies. Some firewalls can also inspect packets and make transformation and security decisions; therefore they are critical components in maintaining security in organizations. There are different types of firewalls such as hardware, software, enterprise, and personal firewalls. Personal firewalls are client-based solutions that are installed on desktop/laptop computers and may be administered individually from a central location. Successful selection and adoption of firewalls (enterprise as well as personal) is based on various factors, some of which are technical while others may be behavioral. This exploratory study looks at the new genre of personal firewalls, and based on review of the literature attempts to identify factors that could result in successful selection of personal firewalls in organizations and further provide empirical evidence to support deployment of firewall software.

The purpose of this paper is to investigate self-referent perceptions of end users, and use Q-Sort analysis to investigate factors affecting deployment of security firewall software in organizations. The paper is organized as follows: Review of research on information security is presented to the reader along with extraction of variables from the literature that may determine firewall deployment in organizations. The Q-Sort Factor Analysis method used for the study is explained and the research design is provided. Along with data analysis, results of the study are then explained, which is followed by discussion and applications to practice. Due to the nature of research design used in this study, limitations are also explained. The study also sheds light on behavioral aspects of information security which may be tied to perceptions of end users who may influence

technology selection in their organization. This will provide empirical evidence to an area which has been identified as lacking in research (Dhillon and Blackhouse, 2001; Troutt, 2002) and provide directions and guidance for future studies.

INFORMATION SECURITY RESEARCH

In the area of information security, research has often lagged practice. Dhillon and Blackhouse (2001) have stressed the need for “more empirical research to develop key principles for the prevention of negative events and therefore to help in the management of security”. Despite known vulnerabilities in applications and operating systems, companies continue to deploy software to stay competitive, and steps taken to secure products and services are knee-jerk reactions to media stories that are more reactive than proactive in nature. Most IT managers lack a coherent framework and concrete methodology for achieving enterprise security. A security plan that includes technology, personnel, and policies would be a much better approach to developing an enterprise security strategy. One such model is the Enterprise Security Framework Price Waterhouse Coopers (PWC) model. The PWC model is comprehensive because it addresses the entire enterprise of security architecture. The model emphasizes information security strategies within the organization using a holistic rather than a piecemeal approach. The framework is based on four pillars: Security Vision and Strategy, Senior Management Commitment, Information Security Management Structure, and Training and Awareness. Within the pillars are Decision Drivers, Development, and Implementation phases. Firewalls are placed in the Development phase since they are used to provide interpretation of corporate standards at the technical level. For a detailed discussion of the PWC model, the reader is referred to Murphy, Boren, and Schlarman (2000).

Firewalls can be considered a last line of defense in protecting and securing information systems. Wood (1988) provided a context for information security systems planning and proposed that reactive and incremental improvement approaches to address security are harbingers of a more serious problem. Other factors identified in Wood’s model are the lack of top management support, information overload, insufficient

staffing, and limited resources. Straub and Welke (1998) advocate using deterrence, prevention, detection, and recovery security action cycle to mitigate systems risk and use prioritized security controls. Data on computer crimes is often underreported because companies are not willing to risk public embarrassment and bad publicity. Most companies choose to handle these incidents internally without keeping documentation or reporting to local, state or federal authorities (Saita, 2001). There is a need for un-biased empirical studies in the information security area that will provide insight into problems affecting today's technology dependent corporations and industries. With a strong need to collect and analyze computer security data, the CSI/FBI Computer Crime and Security Survey is published yearly (see <http://www.gocsi.com>). This study provides descriptive statistics but does not attempt to identify relationship between variables as is expected in analytical surveys. Also, results reported in this annual survey have been identified by the publishers themselves to be potentially misleading due to the limited number of respondents and their accuracy as a result of anonymous nature of the surveys. These results have also been called into question because of lack of statistical or scholarly rigor and self-serving interest (Heiser, 2002). Despite these limitations, the CSI/FBI survey provides a useful role in comparison of yearly data for similar parameters.

To provide better evidence of factors that affect deployment of technology tools that create awareness of security issues and produce better informed employees, research into behavioral factors also needs to be conducted to gain insight into programs and processes that will lead to the development of a robust enterprise security strategy. Information security awareness research has been mostly descriptive and has not explored the possibilities offered by motivation/behavioral theories, or the related theory of planned behavior and the technology acceptance model specifically in the information security domain (Mathieson, 1991; Siponen, 2000; Legris, Ingham, and Collerette, 2003). Since security has been deployed at the perimeter of electronic network and on servers by system administrators, the area of information security has ignored users of information systems since software developers are far removed from how the user will interact with security software. Human compliance with information security rules require an understanding of how people work and think (Highland, 1993). Lane (1985) considers

the human factor to be the first and most important component of security and a critical part of the risk analysis process. This is especially true in personal firewall software since the burden of maintaining a secure environment is being shared by the user and the system administrator.

The area of Human Computer Interface provides a link between the user and software applications. User satisfaction is a function of features, user interface, response time, reliability, installability, information, maintainability, and other factors. “If a product’s user interface catches a user’s attention and is simple to learn and use, and has the right price and features, then the product may gain competitive advantage” (Torres, 2002, p. 15). The theory of user interface design and user involvement in completing tasks based actions related to Internet and security software has been substantiated by two studies in which user interaction with peer-to-peer software (Good and Kerkelberg, 2002), and PGP software (Whitten and Tygar, 1999) were examined. Good and Kerkelberg (peer-to-peer study) found that applications connecting to the Internet need better usability and software design to maintain integrity of information stored on a user’s computer. In this study, individuals assumed responsibility of keeping firewalls operational at all times. This contributed in large part to maintaining effective enterprise security. Whitten and Tygar (PGP study) found that user errors are a significant portion of computer security failures, and further concluded that user interfaces for security programs require a usability standard much different from other consumer software. (Although this study is not directly concerned with user satisfaction, but is more focused on factors that affect deployment rather than development of end-user software in a specific area, some factors may be directly tied to user satisfaction as will be shown by correlational analysis).

An important reason to look at end user perceptions is that it may affect how well the user does his or her part in staying vigilant to combat threats posted by hackers to organizational assets. The end user may be a conduit to organizational data being compromised. Proper software selection as well as positive user attitude and motivation for using the software are therefore important to ensure ongoing use of personal firewall

software. Kettinger and Lee (2002) address the fact that the proliferation of personal computing and individualized software, and popularity of the Internet in organizations have resulted in users playing an important role in driving IT implementation. Their study found that for users selecting their own IT applications (such as desktop software programs), there is greater user satisfaction after implementation. Grantham and Vaske (1985) also state that positive user attitudes are important predictors in continued system use. This is especially important for personal firewall use because computers are at risk at all times when connected to the Internet. In reference to software selection, Chiasson and Lovato (2001) emphasize, "Understanding of how users form perceptions of software innovation would help software designers, implementers and users in their evaluation, selection, implementation and ongoing use of software. However, with the exception of some recent work, there is little research examining how a user forms his or her perceptions of innovation over time" (p. 16). The area of information security as it relates to maintaining confidentiality and integrity of data stored on personal computers can benefit from identification of factors that would make it possible to safeguard corporate assets that are at risk as a result of remote data access by employees. Software selection for deployment on company computers cuts across different user levels in terms of knowledge and level of expertise of the user. Selection of software therefore must be done to accommodate all types of users ranging from novices to experts. The latter category of users may have higher tacit knowledge of tasks to be able to compensate for the interface without realizing it (Gery, 1997).

Due to increasing mobile and off-site access by employees using cable modems, DSL connections, and wireless devices to access corporate resources, personal firewalls are a necessary component to maintain overall enterprise security in an organization. Because of the nature and availability of personal firewall software, most companies choose to acquire it rather than develop it in-house. Software acquisition that results in productivity gains and strategic advantage is of critical concern to organizations, and factors that relate to these benefits must be correctly identified and understood for software acquisition decisions (Nelson, Richmond, and Seidmann, 1996). Purchase of commercial software includes identifying requirements, evaluating packages from

different vendors, configuring, installing, and evaluating it either as server or client-based solution. This may further involve requirements acquisition that leads to product selection (Maiden, Ncube, and Moore, 1997). As a method of selection, professionals in charge of evaluating personal firewall software could draft a feature requirements document, and evaluate vendor products by comparing available features as well as using demonstration versions of software. This would be followed by user experience with the software. As mentioned earlier, the need for user involvement in information systems has been considered an important mechanism for improving system quality and ensuring successful system implementation. It is further believed that the user's satisfaction with a system leads to greater system usage (Baroudi, Olson, and Ives, 1986). The requirements for software though must be as measurable as possible to enable product selection and may also use repertory grids in which stakeholders are asked for attributes applicable to a set of entities and values for cells in an entity-attribute matrix. This would produce representation of requirements in a standardized, quantifiable format amenable even to statistical analyses (Maiden, Ncube, and Moore, 1997). In relation to the security area, Goodhue and Straub (1991) found company actions and individual awareness to be statistically significant in a study of perceptions of managers regarding controls installed in organizations.

RESEARCH DESIGN

Subjects in this exploratory research study were 31 MBA students enrolled in a Security and Control of Information Systems course. The students came from a different background such as finance, liberal arts, nursing, and computer science. From a business perspective, the course examined implications of information security risks faced by organizations. Although technical issues of security such as authentication, authorization, and encryption that make electronic commerce sites successful in processing business transactions securely were also explored in the course, the primary focus in the course was from a business perspective. There was no structured lab work during class, but to gain a better understanding of security issues, students were expected to complete hands-on exercises outside class. During initial weeks, topics covered included the PWC model, TCP/IP vs. OSI models, network, email, database security, digital certificates and

signatures, risk assessment, and privacy issues. Also, during Week 5, students had been previously tested on the above topics using short-answer type questions to determine learning competency of factual information and applications related to information security in organizations. The test score counted towards 15% of overall course grade. With coverage of above topics, it was safe to assume that students had knowledge of current security issues facing organizations in today's economy. Because there is no consensus on the Common Body of Knowledge acceptable for all security professionals, and since this was an exploratory study, the study was conducted in a controlled environment with a homogenous population of students to minimize confounding by extraneous variables. Using MBA students as surrogates for professionals or executives in reference to use and evaluation of technology has also been found to be acceptable (Briggs, Balthazard, Dennis, 1996).

The hands-on firewall assignment in this course covered installation, configuration, and use of one standard personal firewall software (ZoneAlarm). After students had a chance to use the software, they were asked to participate in the study. No class discussion was conducted on results of the firewall tests in case it affected students' perceptions about the software, which could have influenced their response. Therefore, the data reflected individual student perception without class discussions. Students were given instructions to visit a web site that explained the nature of the study and provided information on how the Q-sort statements should be sorted. This was important since students are more used to completing questionnaires in a survey format that use Likert scale, open-ended, or close-ended questions (such as those used during end of term class evaluation of instruction), but may not be familiar with the peculiarities of the Q-sort procedure. To reduce data errors and extract usable data, instructions were presented in detail before the respondents were shown the statements for the study. This was an exploratory study for the purpose of investigating and contributing to research in the relatively new domain of user-centered security products that are being deployed by businesses to increase enterprise security.

Q-Sort Analysis

Q-sort analysis uses a technique for studying human subjectivity (Stephenson, 1953; Brown, 1980; McKeown and Thomas, 1988). It is useful in exploratory research and a well-developed theoretical literature guides and supports its users (Thomas and Watson, 2002). Q-sort methodology is suited for small samples and relies on theories in the domain area being researched to develop items for analysis. A disadvantage of the Q-sort methodology is that it is not suitable for large samples, and it forces subjects to conform to certain expectations (such as fitting responses within a normal distribution). Brown (1986) suggests that 30 to 50 subjects are sufficient for studies investigating public opinion. Q-sort uses an ipsative (self-referenced) technique of sorting participant's statements about subjective conditions. It is a variation of factor analysis technique that uses Q-methodology theory to analyze correlation measure (Brown, 1980). Respondents to a Q-sort studies are required to sort statements into predefined normal distribution type scale in which a fixed number of items fall under each category. The rankings provide clusters of perceptions of individuals' consensus and conflict, which can be used to place individuals with similar characteristics into groups for further study. In the past, the Q-sort technique used index cards for sorting, but now web based data collection programs (such as WebQ) are common. Initially the statements are presented to respondents in random order, and each respondent organizes statements into predefined categories. To view entered data, the respondent also can update statement rankings to see where the statements fall under each category. One advantage of using the WebQ method is that data submission errors are reduced since the program verifies that the statements are sorted according to predefined requirements.

In this personal firewall study, the statements were to be classified by respondents as "Most Important" (+2), "Important" (+1), "Neutral" (0), "Less Important" (-1), and "Least Important" (-2). To provide a forced distribution that is expected in the Q-Sort methodology, respondents were given instructions to identify one statement as "Most Important", two statements each as "Important" and "Less Important", and three statements as "Neutral". The instrument used is shown in Figure 1.

+2		-2	-1	0	+1	+2
+1		-2	-1	0	+1	+2
0		-2	-1	0	+1	+2
	7. Intrusion Reports generated by the firewall software	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
	4. Performance of the product	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
	2. Number of features in the product	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
	6. Regular Product Updates	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
	1. Cost of the desktop firewall	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
	8. Setup and configuration after product has been installed	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
	3. Ease-of-use of the product	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
	9. Availability of Online Help/Technical support	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
	5. Initial Installation of the product	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
-1		-2	-1	0	+1	+2
-2		-2	-1	0	+1	+2

Figure 1: WebQ questionnaire

DATA ANALYSIS

Q-Sort analysis is a type of inverse factor analysis in which the cases (subjects) rather than statement variables (features) are clustered. As recommended by Brown (1980), a procedure that arranged statements based on responses of a single individual was used for data analysis. The responses involved statements of opinion (also called Q-sample) that individuals rank-ordered based on the feature requirements in personal firewall software. The arrayed items (Q-sort) from the respondents were correlated and factor-analyzed. The factors indicated clusters of subjects who had ranked the statement in the same fashion. Explanation of factors was then advanced in terms of commonly shared attitudes or perspectives.

A review of security literature (Hazari, 2000; Northcutt, McLachlan, and Novak, 2000; Scambray, McClure, and Kurtz, 2001; Strassberg, Rollie, and Gondek, 2002; Zwicky, Cooper, Chapman, and Russell, 2000) was used to extract the following

statement variables relating to requirements in personal firewall software: Performance, ease of use, updates, features, reports, cost, configuration, and support. Operational definition of these variables as it relates to the study are provided below:

Performance [PERF]: Refers to how well the software operates under various conditions (such as high traffic, types of data, port scans etc.)

Ease of Use [EOU]: Refers to usability of the product (such as screen design and layout, access to features using tabs, buttons etc.)

Updates [UPDTS]: Refers to product updates at regular intervals after product has been installed and used

Features [FEATR]: Refers to the number of program options and features available in software

Reports [RPORT]: Refers to Intrusion Reports and log files generated by the firewall software

Cost [COST]: Refers to price paid for the product (either as shrink wrapped package or as a download)

Configuration [CONFIG]: Refers to setup and configuration after product has been installed

Support [SUPPRT]: Refers to availability of online help and technical support either by phone or e-mail

Installation [INSTLL]: Refers to initial installation of the product

Prior to conducting the Q-sort analysis, ranked scores of all participants (before identifying factor groups) on each statement variable were calculated for preliminary descriptive statistics. These are shown in Table 1 (Mean Score: 5= Most important , 0= Least important).

Variable	Mean	SD
PERF	4.45	0.77
EOU	3.39	1.08
UPDTS	3.23	0.88
FEATR	3.06	0.93
RPORT	3.00	1.03
COST	2.97	1.20
CONFIG	2.55	0.85
SUPPRT	2.35	0.98
INSTLL	2.00	0.89

Table 1: Participant Ranked scores

Correlation between the nine feature variables shows a low level of correlation between statements. This indicates there is a high degree of independence between the statement categories as used in the analysis. This finding is important since it supports the assertion that the statements represent relatively independent factors obtained from the review of the literature.

	COST	FEATR	EOU	PERF	INSTLL	UPDTS	RPORT	CONFIG	SUPPRT
Cost	1.00	-0.21	0.27	-0.18	-0.13	-0.43*	-0.49*	-0.08	-0.10
FEATR		1.00	-0.29	0.35	-0.16	0.06	-0.17	-0.13	-0.25
EOU			1.00	-0.44*	0.00	-0.37*	-0.27	-0.20	-0.04
PERF				1.00	-0.10	-0.11	-0.13	0.13	-0.14
INSTLL					1.00	-0.13	-0.04	0.18	-0.53*
UPDTS						1.00	0.26	-0.30	0.17
RPORT							1.00	-0.15	0.03
CONFIG								1.00	-0.24
SUPPRT									1.00

Table 2: Correlation matrix between variables

In the correlation matrix shown above, Table 2 shows significant correlation ($p < .05$) between cost and updates, cost and reports, ease-of-use and performance, ease-of-use and updates, and installation and support.

As mentioned earlier, in Q-factor analysis, the correlation between subjects rather than variables are factored. The factors represent grouping of people with similar patterns of response during sorting (Brown, 1980; Thomas and Watson, 2002). Following guidelines for Q-factor analysis, eight factors were initially identified with eigenvalues > 1 (eigenvalue is the amount of variance in the original variable associated with the factor). These factors and their percentage of variance is shown in Table 3.

	Eigenvalues	%	Cumul. %
1	11.56	37.28	37.28
2	6.03	19.45	56.73
3	3.91	12.61	69.34
4	2.98	9.61	78.95
5	2.14	6.92	85.87
6	1.93	6.23	92.10
7	1.43	4.61	96.71
8	1.02	3.29	100.00

Table 3: Eigenvalues of unrotated factors

Factors selected were rotated to maximize the loading of each variable on one of the extracted factors while minimizing loading on all other factors. Factor selected for rotation are usually identified by taking those with eigenvalue greater than one (Kline, 1994). However, in this study, the more rigorous Kaiser rule of selecting factors whose eigenvalue is at or above the mean eigenvalue (in this case 3.85) was used. Factors 1, 2, and 3, which represented almost 70% of total variance in data, were then subjected to principal component analysis with varimax rotation.

Following rotation, a Factor Matrix indicating defining sort (i.e. respondents in agreement) identified three factor groups with similar pattern of responses. The correlation of individual respondents with factors is shown in Table 4.

Factor Loadings			
Q-Sort	1	2	3
1	0.2386	-0.0398	0.8988
2	0.0227	0.1971	0.8158*
3	0.4975	-0.3790	0.5458
4	0.8575*	-0.2912	0.0811
5	-0.2639	0.0196	0.7993*
6	-0.0614	0.7524*	-0.2289
7	0.4014	-0.1587	0.4678*
8	0.1367	0.0728	0.9054*
9	0.5351	0.1183	0.6886*
10	0.5065	0.5665*	0.1764
11	0.5351	0.1183	0.6886
12	0.8192*	0.3263	0.1035
13	0.6495*	0.3357	-0.0844
14	-0.0464	0.7321*	0.5845
15	0.6535*	0.3450	0.3053
16	0.2052	0.8598*	0.2453
17	-0.1340	0.0127	0.9512
18	0.7553*	0.2324	0.2987
19	0.2431	0.4049	0.6946
20	0.5983*	0.5865	-0.0334
21	0.4660	0.6533*	0.4573
22	0.5672*	0.1057	-0.3342
23	0.3501	-0.1001	0.8185
24	0.1008	0.9240*	0.0038
25	0.3329	0.0999	0.2194
26	0.2254	0.6545*	0.1329
27	0.7660*	0.1246	0.5677
28	-0.1210	-0.3611*	0.2307
29	0.3850	0.7032*	0.0144
30	0.4656	0.5605	-0.3196
31	-0.1987	0.8988*	0.2470
% explained variance	21	22	26

Table 4: Factor matrix of respondents (* indicates defining sort)

From the above table it can be observed that for Factor 1, respondents 4, 12, 13, 15, 18, 20, 22, and 27 were in agreement and are highly loaded on this factor. Similarly, respondents 6, 10, 14, 16, 21, 24, 26, 29, and 30 were in agreement in Factor 2, and respondents 5, 7, 8, 9, 11, 17, 19, and 23 were in agreement in Factor 3.

The statements in which these three factor groups were ranked is shown in Table 5.

No.	Statement	Factor 1		Factor 2		Factor 3	
1	COST	0.31	5	0.91	2	-1.45	9
2	FEATR	-0.45	7	0.10	5	0.70	2
3	EOU	0.91	2	0.63	3	-0.55	6
4	PERF	1.26	1	1.72	1	1.80	1
5	INSTLL	-1.92	9	-0.31	6	-0.63	7
6	UPDTS	0.52	3	-0.54	7	0.61	3
7	RPORTS	0.03	6	-1.28	8	0.55	4
8	CONFIG	-1.07	8	0.12	4	-0.17	5
9	SUPPRT	0.41	4	-1.34	9	-0.87	8

Table 5: Ranked statement totals with each factor

Table 6 shows correlation between the factors. Similar to the findings earlier about variable independence, the factor groups also show a high degree of independence.

Factor	1	2	3
1	1.0000	0.3218	0.2970
2	0.3218	1.0000	0.2298
3	0.2970	0.2298	1.0000

Table 6: Correlation between factors

The normalized factor scores for each factor were examined next. This provided a measure of relative strength of importance attached by a factor to each statement on the scale used during sorting. Tables 7a, 7b, and 7c show these scores.

No.	Statement	z-score
4	PERF	1.258
3	EOU	0.910
6	UPDTS	0.524
9	SUPPRT	0.409
1	COST	0.314
7	RPORT	0.032
2	FEATR	-0.454
8	CONFIG	-1.071
5	INSTLL	-1.922

Table 7a: Normalized Factor 1 score

From the above table it can be seen that adherents of Factor 1 feel strongly in favor of statement 4 (Performance) and oppose statements 8 and 5. This indicates for Factor 1 group, performance is preferred over initial installation, setup and configuration of the product.

No.	Statement	z-score
4	PERF	1.717
1	COST	0.905
3	EOU	0.626
8	CONFIG	0.116
2	FEATR	0.102
5	INSTLL	-0.313
6	UPDTS	-0.535
7	RPORT	-1.276
9	SUPPRT	-1.343

Table 7b: Normalized Factor 2 score

The results of Factor 2 group are consistent with Factor 1, i.e. Performance of the product is the highest rated criterion. Ease of use also rated highly in Factors 1 and 2. Perceived ease of use in an information systems product has been shown to play a critical role in predicting and determining a user's decision to use the product (Hackbarth, Grover, and Yi, 2003). The largest dissension between Factor 1 and 2 groups involved statements 9 (Availability of online help), 7 (Intrusion reports generated), and 6 (Regular product updates).

No.	Statement	z-score
4	PERF	1.805
2	FEATR	0.702
6	UPDTS	0.606
7	RPORT	0.553
8	CONFIG	-0.170
3	EOU	-0.547
5	INSTLL	-0.632
9	SUPPRT	-0.872
1	COST	-1.446

Table 7c: Normalized Factor 3 score

The results of Factor 3 are consistent with Factors 1 and 2 with Performance criteria once again being highly rated. The most dissension between Factors 2 and 3 involved statements 1 (Cost) and 3 (Ease of use). The most dissension between Factors 1 and 3 involved statements 1 (Cost), 3 (Ease of use), and 9 (Availability of online help).

DISCUSSION AND APPLICATIONS FOR PRACTICE

The Q-sort analysis classified subjects into three groups. Eight subjects were classified under Factor 1, and 10 subjects each were included in Factors 2 and 3. There were three subjects in the study that were not distinguished in any group. These subjects were excluded from further analysis. The classification into factors gave a better idea of group characteristics. Since Factors 1 and 2 were similar and shown to include subjects who considered performance, ease of use, and availability of online help as the most important characteristics, this group can be considered to be comprised of non-technical users who place more emphasis on the product performing as expected in achieving goals for security. Factor 3 subjects emphasized technical characteristics and were more interested in number of features in the product, updates to the product on a regular basis, intrusion reports generated by personal firewalls, and setup/configuration of the product after installation. This group had characteristics of technical users.

The normalized factor scores provided a measure of relative strength of importance attached by factors to each statement on the scale used during sorting. As mentioned earlier, adherents in Factor 1 felt strongly in favor of statement 4 (Performance) and opposed statements 8 (Setup/configuration) and 5 (Installation). The results of Factor 2 are consistent with Factor 1, i.e. Performance of the product is the highest rated criterion. Ease of use also rated highly in Factors 1 and 2. The largest dissension between Factor 1 and 2 groups involved statements 9 (Availability of online help), 7 (Intrusion reports generated), and 6 (Regular product updates). The most dissension between Factors 2 and 3 involved Statements 1 (Cost) and 3 (Ease of use). Results of Factor 3 were consistent with Factors 1 and 2, with Performance criteria once again being highly rated. The largest dissension between Factors 1 and 3 involved

statements 1 (Cost), 3 (Ease of use), and 9 (Availability of online help). Extreme differences between all factors appeared in Cost, Intrusion Reports generated, and Availability of online help. There was only one statement, Performance of the product, that showed consensus among all factors i.e. it did not distinguish between any pair of factors which indicates Performance of the desktop firewall software is an agreed upon criterion irrespective of group characteristics.

The managerial implications of this study can be assessed at the level of selecting appropriate software for use on computers in organizations to maintain security. There is evidence of user satisfaction being a useful measure of system success (Mahmood et. al, 2000). While the end user may not purchase individually preferred software for installation on company owned computers, the user can influence decisions for selection by making known to IS managers the features that would contribute to regular use of security software such as personal firewalls. Given access of these machines to corporate resources, appropriate and regular use of software would contribute to maintaining enterprise security. For technical professionals (e.g. programmers) who install firewalls on their desktop, programs could emphasize the statements that are defining characteristics shown in Factor 3. For an industry that has non-technical professionals (such as Factor 1 and 2), other non-technical characteristics of the product could be emphasized thus achieving maximum effectiveness in program deployment. Increased awareness should minimize user related faults, nullify these in theory, and maximize the efficiency of security techniques and procedures from the user's point of view (Siponen, 2000).

The results of this study could also benefit vendors who develop software for end users. In this study it was found that performance of the software is the most important factor that affects selection of software, irrespective of group characteristics. Due to project deadlines and market competition, software is often shipped without being fully tested as secure, and standard industry practice is to release incremental service packs that address security issues in the product. In a case of security software, this may adversely affect the reputation of a vendor once its products have been shown to have

high vulnerability to being compromised. The findings of this study could provide a better understanding of importance of personal firewall security software on organizational client computers. The decision to install an information system necessitates a choice of mechanisms to determine whether it is needed, and once implemented, whether it is functioning properly (Ives, Olson, and Baroudi, 1983). More research needs to be done in the area of selection of software for implementation on user's computers that are owned by corporations and given to employees for off-site work. This can include regular employees versus contractors who may connect to employer and client networks from the same computer. If the findings are to have wider applicability, qualified industry professionals and security officers responsible for maintaining secure infrastructure in corporations should be included in the analysis. The study provides management and security professionals a basis for making decisions related to enterprise security. It provides personal firewall vendors an insight into feature requirements of the personal firewall market, and provides academic researchers interested in security, a more focused approach on various dimensions of security software from the behavioral perspective. Future studies could be industry and product specific in order to assess differences in selecting general-purpose software versus security specific products.

In many cases, management has looked at the need for implementing information security programs and products as a necessary encumbrance, something akin to paying taxes or insurance premiums (Highland, 1993). But organizations are increasingly becoming aware of the potential for legal exposure via lawsuits, and are deploying countermeasures (such as personal firewalls) to reduce vulnerability and mitigate risk. The chief information security officer in today's organizations should have the responsibility of managing organizational risks by using empirical models and analysis to determine strategies for protecting corporate assets. Firewalls are the last line of defense in the corporate network and therefore play a critical role in information security. With personal firewalls being a new product genre, this study was conducted since there is no research available that specifically looks at determinants for selection of security software in a corporate environment to protect organizational assets. As the information

security field evolves further, decisions for security software acquisitions need to be researched further. Selection and deployment of appropriate firewalls can make a significant difference in an organization's enterprise security strategy. It is therefore also important to understand the variables (as shown in this study) that may affect decisions to select and deploy personal firewall software in a corporate environment.

LIMITATIONS OF THE STUDY

Due to the exploratory nature of this study, there are several limitations. The sample used in the study comprised of all students enrolled in a security course at the same university, and was further limited to the firewall topic among a wide range of technical and behavioral information security topics. Students worked with only one type of firewall software and characteristics of this particular program may have heightened their awareness of certain strengths and weaknesses in the software. Since the purpose of information security implementation in an organization is to support business objectives of the organization, information security departments are sometimes placed under the chief financial officer recognizing the direct relationship between information assets and monetary assets. Software acquisition decisions may therefore be made by the finance department with limited input from the IT department. The purpose of this study was to explore an important topic for research on information security and determine operant subjectivity in a field where empirical research is severely lacking. The Q-sort technique itself is suitable for small sample populations (Thomas and Watson, 2002) but the correlations obtained in smaller samples tend to have considerable standard errors (Kline, 1994). The exploratory nature of this study was not intended to prove some general proposition but to seek a better understanding of group characteristics that directly relate to maintaining a secure network environment (in this case by deploying personal firewalls to plug possible vulnerabilities that might exist in a network through use of computers by employees either on-site or at remote locations). The perceptions of end users will therefore guide the selection and deployment of security technologies in an organization to provide a secure corporate environment.

CONCLUSION

In this study, Q-methodology was used to define participant viewpoints and perceptions, empirically place participant in groups, provide sharper insight into participant preferred directions, identify criteria that are important to participants, explicitly outline areas of consensus and conflicts, and investigate a contemporary problem relating to desktop firewalls by quantifying subjectivity. Similar to other IT areas, security software selection and deployment in today's environment faces many challenges such as staying current with new threats, project deadlines, implementation issues, and support costs. Quality drives customer satisfaction and adoption of software. Human factors are important in contributing to successful software deployment in organizations, especially when it relates to desktop software applications. Organizations are now viewing security and controls as business enablers and desktop firewall technology plays a critical role in safeguarding corporate assets. In a fast-paced area where the new generation of applications and services are growing more complex each day, it is critical to understand characteristics that affect selection of end user security products in enterprises.

This study addresses a small but important area of safeguarding enterprise information security by using personal firewalls. As has been previously noted, limited research exists beyond the current study that explores behavioral aspects of information security. This study holds importance for professionals tasked with evaluating and selecting security products for company wide deployment. As the area of information security gains increased importance due to the strategic role of technology in organizations, and current events impact areas such as disaster recovery and enterprise continuity planning, a study of end users to determine their perceptions about selection of technology controls in organizations is critical for protecting organizational assets. More research needs to be done in the area of perception of users towards other security software (such as anti-virus, intrusion detection, virtual private network software, and encryption products), and due to varying security needs in different industries; studies could also be industry and product specific. While the findings should be considered preliminary, the results raise interesting observations about issues uncovered regarding

security perceptions of feature requirements in personal firewalls. Information security is a dynamic area and in this environment, this exploratory study contributes to evolving research by identifying variables from theoretical literature and using an empirical technique to study issues that affect safeguarding vital assets of an organization from internal and external threats.

REFERENCES:

- Baroudi, J., Olson, M., & Ives, B. (1986). An empirical study of the impact of user involvement on system usage and information satisfaction. *Communications of the ACM*, 29(3), 785-793.
- Briggs, R. O., Balthazard, P.A. & Dennis, A. R. (1996). Graduate business students as surrogates for executives in the evaluation of technology. *Journal of End User Computing*, 8(4), 11-17.
- Brown, S. R. (1980). *Political subjectivity: Applications of Q methodology in political science*. CT: Yale.
- Brown, S. R. (1986). Q-technique and method: Principles and procedures. In W. D. Berry & M. S. Lewis-Beck (Eds.), *New tools for social scientists: Advances and applications in research methods*. Beverly Hills, CA: Sage Publications.
- Chiasson, M. & Lovato, C. (2001). Factors influencing the formation of a user's perceptions and use of a DSS software innovation. *ACM SIGMIS Database*, 32(3), pp. 16-35.
- Clarke, R. (2002, February). *Forum on Technology and Innovation: Sponsored by Sen. Bill Frist (R-TN), Sen. Jay Rockefeller (D-WV), and the Council on Competitiveness*. Retrieved October 28, 2003, from: <http://www.techlawjournal.com/security/20020214.asp>
- Deise, M., Nowikow, C., King, P., & Wright, A. (2000). *Executive's guide to e-business: From tactics to strategy*. New York: John Wiley & Sons.
- Dhillon, G. & Blackhouse, J. (2001). Current directions in IS security research: Toward socio-organizational perspectives. *Information Systems Journal*, 11(2), 127-153.
- Enns, H., Huff, S., & Golden, B. (2003). CIO influence behaviors: The impact of technical background. *Information and Management*, 40(5), 467-485.
- Gery, G. (1997). Granting three wishes through performance-centered design. *Communication of the ACM*, 40(7), pp. 54-59.
- Good, N. & Krekelberg, A. (2002). *Usability and privacy: a study of Kazaa P2P file-sharing*. Retrieved November 12, 2003, from <http://www.hpl.hp.com/shl/papers/kazaa/>
- Goodhue, D.L. & Straub, D.W. (1991). Security concerns of system users: A study of perceptions of the adequacy of security measures. *Information & Management*, 20(1), 13-27.

Grantham, C. & Vaske, J. (1985). Predicting the usage of an advanced communication technology. *Behavior and Information Technology*, 4(4), 327-335

Hackbarth, G., Grover, V., & Yi M., (2003). Computer playfulness and anxiety: positive and negative mediators of the system experience effect on perceived ease of use. *Information and Management*, 40 (3), 221-232.

Hazari, S. (2000). *Firewalls for beginners*. Retrieved December 17, 2003, from <http://online.securityfocus.com/infocus/1182>

Heiser, J. (2002, April). Go figure: Can you trust infosecurity surveys? *Information Security*, 27-28.

Highland, H. J. (1993). *A view of information security tomorrow*. In E. G. Dougall (ed.), *Computer security*. Holland: Elsevier.

Ives, B., Olson, M., & Baroudi, J. (1983). The measurement of user information satisfaction. *Communications of the ACM*, 26(10), 785-793.

Kettinger, W. & Lee, C. (2002). Understanding the IS-User divide in IT innovation. *Communications of the ACM*, 45(2), pp. 79-84.

Kline, P. (1994). *An easy guide to factor analysis*. London: Rutledge

Lane, V. P. (1985). *Security of computer based information systems*. Macmillan: London.

Legris, P., Ingham, J., & Colletette, P. (2003). Why do people use information technology? A critical review of the technology acceptance model. *Information and Management*, 40(3), 191-204.

Mahmood, M. A., Burn, J. M., Gemoets, L. A., & Jacquez, C. (2000). Variables affecting information technology end-user satisfaction: A meta-analysis of the empirical literature. *International Journal of Human-Computer Studies*, 52, 751-771.

Maiden, N., Ncube, C., & Moore, A. (1997). Lessons learned during requirements acquisition for COTS systems. *Communications of the ACM*, 40(12), 21-25.

Mathieson, K. (1991). Predicting user intentions: Comparing the technology acceptance model with the theory of planned behavior. *Information Systems Research*, 3(2), 173-191.

McKeown, B., & Thomas, D. (1988). *Q Methodology*. California: Sage Publications Inc.

Murphy, B., Boren, R. & Schlarman, S. (2000). *Enterprise Security Architecture*, CRC Press. Retrieved November 2, 2003, from <http://www.pwcglobal.com>

Nelson P., Richmond W. & Seidmann A., (1996). Two dimensions of software acquisition. *Communications of the ACM*, 39(7), 29-35.

Northcutt, S., McLachlan, D., & Novak, J. (2000). *Network intrusion detection: An analyst's handbook* (2nd Ed.). IN: New Riders Publishing.

Saita, A. (2001, June). Understanding peopleware. *Information security*, 72-80.

Scambray, J., McClure, S., & Kurtz, G. (2001). *Hacking exposed* (2nd Ed.). CA: Osborne/McGraw-Hill.

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness, *Information Management & Security*, 8(1), 31-41.

Stephenson, W. (1953). *The study of behavior*. Chicago, IL: University of Chicago Press.

Strassberg, K., Rollie, G., & Gondek, R. (2002). *Firewalls: The complete reference*. NY: Osborne McGraw-Hill.

Straub, D.W. & Welke, R. J. (1988). Coping with systems risk: security planning models for management decision making. *MIS Quarterly*, 22(4), 441-469.

Summers, R. (1997). *Secure computing: Threats and safeguards*. New York, NY: McGraw-Hill.

Thomas, D. & Watson, R. (2002). Q-sorting and MIS research: A primer. *Communications of the AIS*, 8, 141-156.

Torres, R. J. (2002). *Practitioner's handbook for user interface design and development*. NJ: Prentice-Hall.

Troutt, M. D. (2002). IT security issues: The need for end user oriented research. *Journal of End User Computing*, 14(2), 48

Whitten, A. & Tygar, J. (1999). Why Johnny can't encrypt: A usability evaluation of PGP 5.0, *Proceedings of the 8th USENIX Security Symposium*.

Wood, C. (1988). A context for information systems security planning. *Computers & Security*, 7(5), 455-465.

Zwicky, E., Cooper, S., Chapman, D, & Russell, D. (2000). *Building internet firewalls* (2nd Ed.). CA: O'Reilly.