Mitigating Information Security Risks by Increasing User Security Awareness: A Case Study of an Information Security Awareness System

Charlie C. Chen

R. S. Shaw

Samuel C. Yang

Organizations that lack security awareness can miss detecting many obvious security risks such as Trojans, phishing, viruses, and intellectual property theft in their daily activities. This lack of awareness can render sophisticated Internet security technologies useless and expose the organization to enormous risks. This paper adopts the systems development research methodology to investigate the security awareness needs of an insurance company that has an e-business presence. A pilot of a security awareness system was constructed for this investigative purpose. Various managers in the organization took part in the study. The pilot system was fine-tuned based on the usage experiences and feedback of participants. The findings indicate that the architecture of an information security awareness system needs to provide effective system management components that allow a system manager to customize the system interface in order to meet individual needs. In addition, the system itself needs to provide different functions such as an information portal, newsgroups, discussion forums, histories of security breach events, security awareness activities, and quality articles to facilitate the transmission of awareness concepts. The results of this study provide important lessons for organizations that plan to implement an effective information security awareness system.

Security is a major concern for organizations that have an e-business presence. Many customers are hesitant to provide their personal information on the Internet due to the lack of privacy (Hoffman, Novak, & Peralta, 1999) and trust (Liu, Marchewka, Lu, & Yu, 2005). From an organization's perspective, a lack of security knowledge and awareness on the part of employees is also a major problem. Numerous security risks, such as viruses, worms, denial-of-service attacks, stolen passwords, social engineering, and authority and authorization violations are the result of a lack of security awareness. These risks are detrimental to the operation of an organization. As such, organizations need to be aware of these risks, dissuade individuals from committing risky acts, and deploy countermeasures such as deterrence, prevention, detection, and recovery.

Information security threats can originate internally or externally by human or non-human perpetrators (Loch, Carr, & Warkentin, 1992). Natural disasters are external threats that are beyond human control, whereas hackers and employee misconduct are controllable external and internal security threats. Internal security

Charlie C. Chen is Assistant Professor, Department of Computer Information Systems, Appalachian State University, Boone, North Carolina.

R. S. Shaw is Associate Professor, Department of Information and Management, Tamkang University, Tamsui, Taiwan.

Samuel C. Yang is Associate Professor, Department of Information Systems and Decision Sciences, California State University, Fullerton, California.

threats include user security errors, security carelessness, security negligence, and security attacks (Leach, 2003). Information systems may be secured by preventing, detecting, and correcting internal and external threats. A lack of security awareness can make an organization vulnerable to these internal and external threats.

Although many organizations have deployed hardware- and software-based protections such as firewalls, proxy servers, anti-virus software, and password management, incorporating these technology-based solutions has not significantly decreased the security risks to organizations. In fact, risks and attacks are evolving to elude many current technology-based protections (Claburn, 2005). According to the 2005 Computer Crime and Security Survey conducted jointly by the Computer Security Institute and the Federal Bureau of Investigation, virus infection is still the most common security risk (73%). Insider abuse is now the second most common security risk (47%), more common than denial of service attacks (32%) (Gordon, Loeb, Lucyshyn, & Richardson, 2005). Today's security problems are primarily due to the inadequate security awareness of users, which can be mitigated without the need for sophisticated security technologies. The human factor in security is more important than technology (Desman, 2003).

In addition, the 2004 E-Crime Watch study surveying security and law enforcement executives found that many respondents do not track losses due to e-crime or intrusions (32%), do not know the total amount of loss even if they do track them (34%), and do not have a formal plan for dealing with e-crimes and intrusions (41%) (United States Secret Service [USSS], Chief Security Officer [CSO] Magazine, & Computer Emergency Response Team [CERT] Coordination Center, 2004). Given that these interviewees are at the executive level of their organizations, their lack of security awareness shows the potential vulnerability of organizations' information infrastructure.

The Department of Trade and Industry's 2004 Information Security Breaches Survey reports that humans are the weakest link in the chain of security control. Thus, one effective preventive measure is to create a security-aware culture by educating staff about security risks and their responsibilities (Timms, Potter, & Beard, 2004). Improving basic knowledge and judgment about sharing information can help prevent human errors and carelessness, but few companies have adequate information security training programs in place to improve security awareness. When asked to rate the level of security awareness in their organizations, 67% of 400 information security officers reported either "inadequate" or "dangerously inadequate" in a security awareness report (Pentasafe Security Technologies, 2002). This result is confirmed by the 2005 Computer Crime and Security Survey that states, "...On average, respondents from all sectors—except the high-tech sector and the federal government—do not believe that their organization invests enough in security awareness." (Gordon et al., 2005, p. 17)

While deploying technological solutions and countermeasures is important in combating security risks (Claburn, 2005), improving the level of security awareness of users and managers is equally if not more important (Timms et al., 2004; Vijayan, 2005). Security awareness programs are often implemented using newsletters, posters, trinkets, and Web sites. The goal of this study is to build an information security awareness system (ISAS) as an artifact and to explore the appropriate functions and usability of an ISAS that aims to improve users' security awareness level. Functions built and investigated include a discussion forum, risks events, awareness activities, a newsletter and article sharing, and a management center. We adopted a systems development methodology to build a pilot system based on users' feedback over a six-month period. Subjects participating in this study are from the foreign subsidiary of an asset management company and consist of two senior information security managers of the risk management department, one training manager of the risk management department, and two assistant managers in the auditing department. We also consider these managers as the users of the pilot system. Interviewing these subjects provides insights about important issues concerning the deployment of an information security awareness system.

Research Methodology

Most information systems (IS) researchers adopt one of four general methodological approaches: theory building, experimentation, observation, or systems development (Nunamaker, Chen, & Purdin, 1991). Each approach complements one another and is appropriate for different research problems. Since security awareness is an emerging field, the systems development approach can help establish the research domain based on a working system because "systems development provides the exploration and synthesis of available technologies that produces the artifact (system) that is central to this process" (Nunamaker et al., 1991, p. 93). In this approach, the feedback of observation and evaluation of a security awareness system is important as problems can be identified, generalized, and overcome. Additionally, continuing technological advancements can help incrementally improve the existing system to gain further insights.

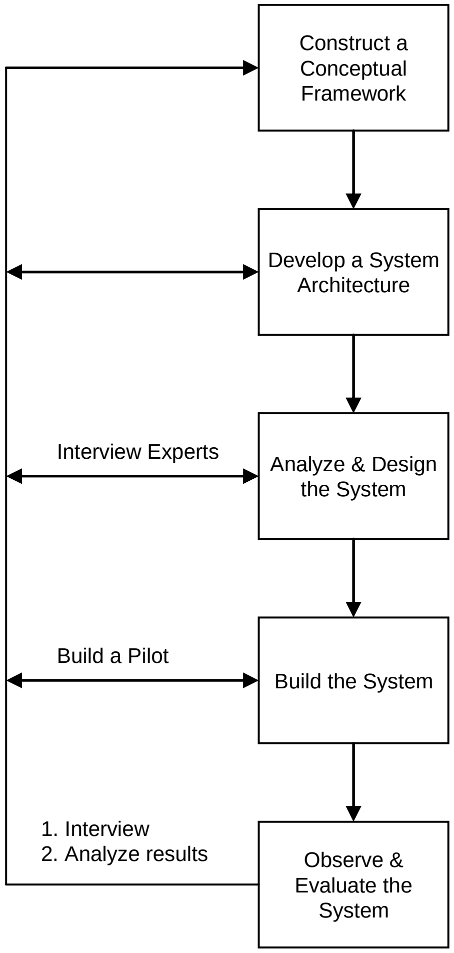
Figure 1 shows the systems development research methodology used by this study. It comprises five steps: 1) construct a conceptual framework; 2) develop a system architecture; 3) analyze and design the system; 4) build a pilot system; and 5) observe and evaluate the system (Nunamaker et al., 1991). Meeting the goal of building an information security awareness system depends on developing a conceptual framework to understand the characteristics of an online security awareness learning system and its functionalities. The system architecture is important because it serves as a top-level structure that guides the development of the system. By examining relevant technologies, information systems researchers can adopt new approaches to analyze and design a more effective system. In addition, throughout the building process IS researchers can gain insights into the system's issues and complexities. Experiences acquired from observing and evaluating the system can be consolidated to help better understand the system and improve future system building efforts, and "implementation of a system is used to demonstrate the feasibility of the design and the usability of the functionalities of a system development research project" (Nunamaker et al., 1991, p. 100). All in all, the functionalities of system components and their interrelationships can be made clearer throughout the system development process (Kast & Rosenzweig, 1972).

Theoretical Background

The National Institute of Standards and Technology (NIST) defines information security "awareness" in the Special Publication 800-16 as follows:

> Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow

Figure 1. System Development Research Methodology (Nunamaker et al., 1991)


Construct a Conceptual Framework
Develop a System Architecture
Interview Experts
Analyze & Design the System
Build a Pilot
Build the System
1. Interview
2. Analyze results
Observe & Evaluate the System

> individuals to recognize IT security concerns and respond accordingly. In awareness activities, the learner is the recipient of information, whereas the learner in a training environment has a more active role. Awareness relies on reaching broad audiences with attractive packaging techniques. Training is more formal, having a goal of building knowledge and skills to facilitate the job performance (1998, p. 15).

This definition shows that security awareness efforts constitute active informing intended to change the behavior of users and reinforce good security practices. Specifically, "awareness relies on reaching broad audiences with attractive packaging techniques." Thus, based on this definition, the question asked by the research is, "What are the characteristics of an information system that increase the awareness of information security in an organization?" To answer this question, an information security awareness system can be built that leverages electronic learning (e-learning) methods to deliver security awareness concepts. This can be done for two reasons. First, an e-learning platform, when designed appropriately, is well-suited to reach a wide employee base in an organization. Second, using modern web and e-learning development tools, content can be attractively packaged in such a way as to "focus attention on security," helping employees to "...recognize IT security concerns and respond accordingly" (NIST, 1998, p. 15).

In terms of e-learning, the American Society for Training and Development (ASTD) defines e-learning as "instructional content or learning experiences delivered or enabled by electronic technology" (2001, p. 7). In terms of the actual learning delivery, e-learning includes strategies such as computer-based learning, web-based learning, and distance learning (ASTD, 2001). In particular:

- Computer-based learning (CBL) has to do with storing course materials on a CD or other media so a person can learn by himself or herself.
- Web-based learning (WBL) is learning via the intranet or the Internet. WBL is sometimes known as online learning.
- Distance learning is a broader term that includes mail and catalog-based learning in addition to using electronic technology.

Although many emphasize the efficiency and lower cost of e-learning and the shortening of the amount of time it takes for workers to learn (ASTD, 2001), organizations should also focus on the effectiveness of learning delivery. Since context is important in online learning, research has been aimed at developing more "attractive and viable" online education approaches in a specific context (Valenta, Therriault, Dieter, & Mrtek, 2001, p. 111). Because employees already function in an organization, situational learning is an effective user-centered learning approach that improves the security awareness of users about their working environment (Endsley & Garland, 2000). In addition, course materials in e-learning can be designed from the perspective of learners and be tailored to the needs of different users (Siponen, 2000). Thus, e-learning in an organizational context is well-suited for learning security awareness concepts because organizational employees in today's environment are required to be security-conscious.

In terms of security awareness, the concept of information security is a multidimensional one that includes authorization, authentication, confidentiality, data integrity, availability, and recovery (Dam & Lin, 1996). The effective communication of security awareness depends on multiple approaches to conveying security awareness messages. The International Organization for Standardization (ISO) 17799 security standard (ISO, 2005) provides a guideline for security experts to make consistent assessments of security awareness of users in an organization. This standard specifies ten awareness topics: 1) information security policy; 2) system access control; 3) system development and maintenance; 4) personnel security; 5) physical and environmental security; 6) security organization; 7) asset classification and control; 8) communications and operations management; 9) business continuity management; and 10) compliance (McAdams, 2004).

Wilson and Hash (2003) assert that a sound ISAS needs to contain interactive course materials. Merely transmitting information about security breach incidents is insufficient. Instead, a user needs to be able to respond to the incidents because doing so can facilitate improving the security awareness of a user and transferring security knowledge. From the perspective of constructivism, a learner can acquire external knowledge and create new knowledge based on his or her prior knowledge and experience and through interacting with the external world (Chen, 2003; Leidner & Jarvenpaa, 1995). Security breach events appear in versatile and unpredictable forms that are difficult to prevent; this difficulty underscores the importance of improving the capability of a user both to be aware and to respond to security threats. The interactive learning approach is fundamental for the success of an ISAS (Furnell, Gennatou, & Dowland, 2002).

An ISAS, furthermore, needs to have the ability to save duration records and usage history. This information is important for the manager of an awareness program to assess how well awareness concepts have been communicated. When security breaches or unusual events occur, an ISAS needs to have the capabilities both for users to report them and for management to act upon them. Management needs to document lessons learned each time issues are resolved, and the documentation constitutes a repository of information of past security events and solutions. Weblog, Wiki, and discussion forums are useful tools for this purpose (Wagner, 2004).

Authentication is another important mechanism when designing an ISAS. Users with different access authorities can access various tiers of information. General users are the targeted users of the security awareness system, so ease of use and common features are important criteria for the design of an ISAS. Webpage editing tools, such as HTML, Frontpage, Dreamweaver MX, or Flash, can facilitate the creation of user-centered content materials.

Based on the discussions thus far, Table 1 depicts a framework of high-level requirements for an ISAS. In addition, Table 1 also shows the commonalities and differences between e-learning systems and an ISAS. In terms of similarities, an intranet and the Internet can be vehicles for both systems to deliver information. Rich and interactive content is a common ingredient of system success. Abilities to record usage history and to personalize course content based on the needs of targeted users are important for these systems.

Table 1. E-Learning vs. Security Awareness System

	Security Awareness systems	E-learning systems
Similarities	• Rich and interactive content • Delivery of content via the Internet or intranet • Users can express opinions • Recording learning process • Managing content • Targeting all levels of employees and customizable	• Rich content • Delivery of content via the Internet or intranet • Students can post messages • Recording learning process • Managing course content • Customizing course content for groups
Differences	• Security awareness focus • Emphasizing employee involvement and effective communication • Multi-methods to establish awareness • Supporting business operations • Tracking usage histories • Diversified feedback methods to improve the program	• Learning focus • Delivery of structured/semi-structured instructional content or learning experiences • Focus on predetermined learning path • Measurement of specific learning outcomes

Although e-learning and security awareness systems have similarities, the two systems are different from each other in terms of their foci, and the salient differences are emphasized here to highlight the unique, important requirements of an ISAS. The main purpose of an e-learning system is to instill users with knowledge about a particular subject (McCrea, Gay, & Bacon, 2000; Wilson & Hash, 2003). Subjects vary with their difficulty and are often in a hierarchical order. The best way to deliver course content in an e-learning system is to present contents in a predetermined learning sequence. This arrangement can also ease the assessment process. However, security awareness concepts have a less defined structure and cannot be easily placed in a presentation order. For example, awareness of password-setting policies does not directly help to improve the awareness level of a user needing to protect physical assets. These are independent topics and should be assessed separately. In addition, a user needs to have the ability to interact with an ISAS via posting opinions, giving information and feedback, and reporting risks or threats to the system.

Auditing is another important feature of an ISAS. This feature can help ensure that the posted records are adequate and accurate and can benefit users of the system. Furthermore, involvement of all employees in the use of ISAS is essential for its success. Different communication modalities, such as e-mails, broadcast messages, newsletters, and reports, can help users become aware of their security situations and should be considered in the design of an ISAS. Lastly, the system needs the flexibility to modify its content materials according to assessment results such as an online test (Furnell, Gennatou, & Dowland, 2002; Siponen, 2000; Wilson & Hash, 2003).

ISAS Pilot System

We conducted this study in the context of an actual organization. The participating organization is the foreign subsidiary of an asset management company. The company is ranked 14th in the top 20 global financial institutions and 17th in the 2005 Global 500 companies (Fortune, 2005). This company operates globally and serves over 11 million online customers in nine countries (New York Stock Exchange [NYSE], 2005). Its foreign subsidiary in Taiwan has major lines of business in banking, finance, and insurance. The company recognizes the increasing cyber security threat and was interested in establishing an IT security awareness program to improve the security awareness of its employees. The company accepted our proposal to customize a security awareness system for it on an e-learning platform. As described above, five managers at the subsidiary, who are also considered users of the pilot system, participated in the study. We built a pilot system and solicited feedback to fine-tune the system. This study reports the system-building process and lessons learned from the project.

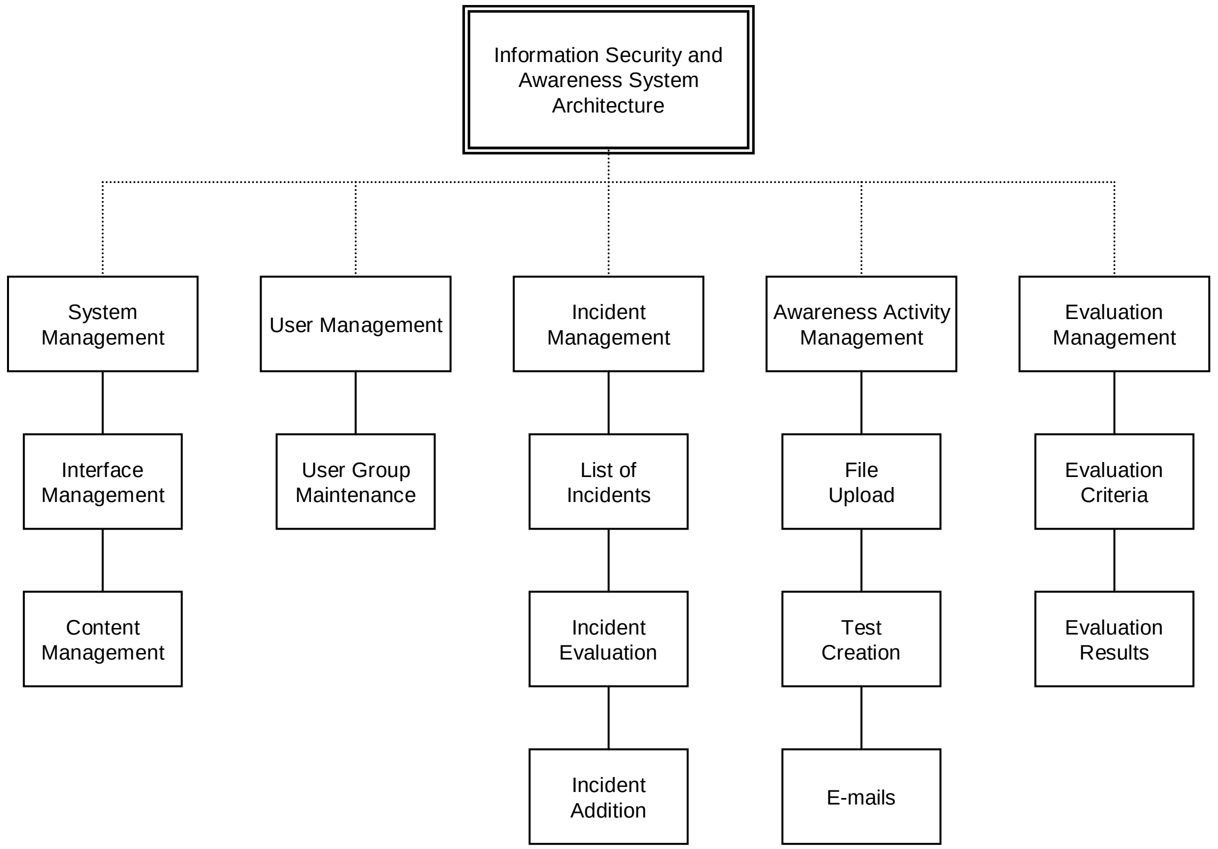
System Functions

To capture the requirements for the ISAS, we interviewed the experts in our participant pool. The experts consist of the two senior information security managers and one training manager of the risk management department. The department is responsible for risk control and the cultivation of a security awareness culture in the company. Based on the requirements gathered, we included five key components in the system architecture that is used to administer the system and to guide the development of the system functions described in the next section. The five components are system management, user management, incident management, awareness activity management, and evaluation management. Figure 2 shows the system architecture and functions, and its five components are described below:

System Management. The system manager can routinely manage system contents such as discussion topics and contents, news, and articles using the system management component. Note that this component is used to manage three major functions of the system: news, discussion, and selected articles. In terms of the interface management, the system manager can use this subcomponent to personalize webpage layouts and authorization rights for each individual.

User Management. This component allows the system manager to maintain users' data and

Figure 2. System Architecture and Functions



confidential information. In doing so, the system manager authorizes and authenticates users based on their user groups (i.e., regular user, power user, and administrator). This component also enables a system manager to store and access user information from a central place.

Incident Management. This component gives the system manager the ability to add, delete, maintain, and manage incident events using wizards and templates. In addition, the system manager needs to evaluate and modify the incident events written by users. After verifying the content, the manager can authorize or decline the publication of specific incidents. This component is used for the major function of administering internal incidents in the system.

Awareness Activity Management. Using this component, the system manager can add and delete awareness activities as well as easily create new projects. For example, a system manager can upload files to the database server so users can browse through activity files. The system manager can also use templates provided to create course content based on users' needs, as well as to create online exams. Lastly, a system manager can send e-mails in HTML format with or without attachments to designated user groups. This component is used for the system function of managing activities within the system.

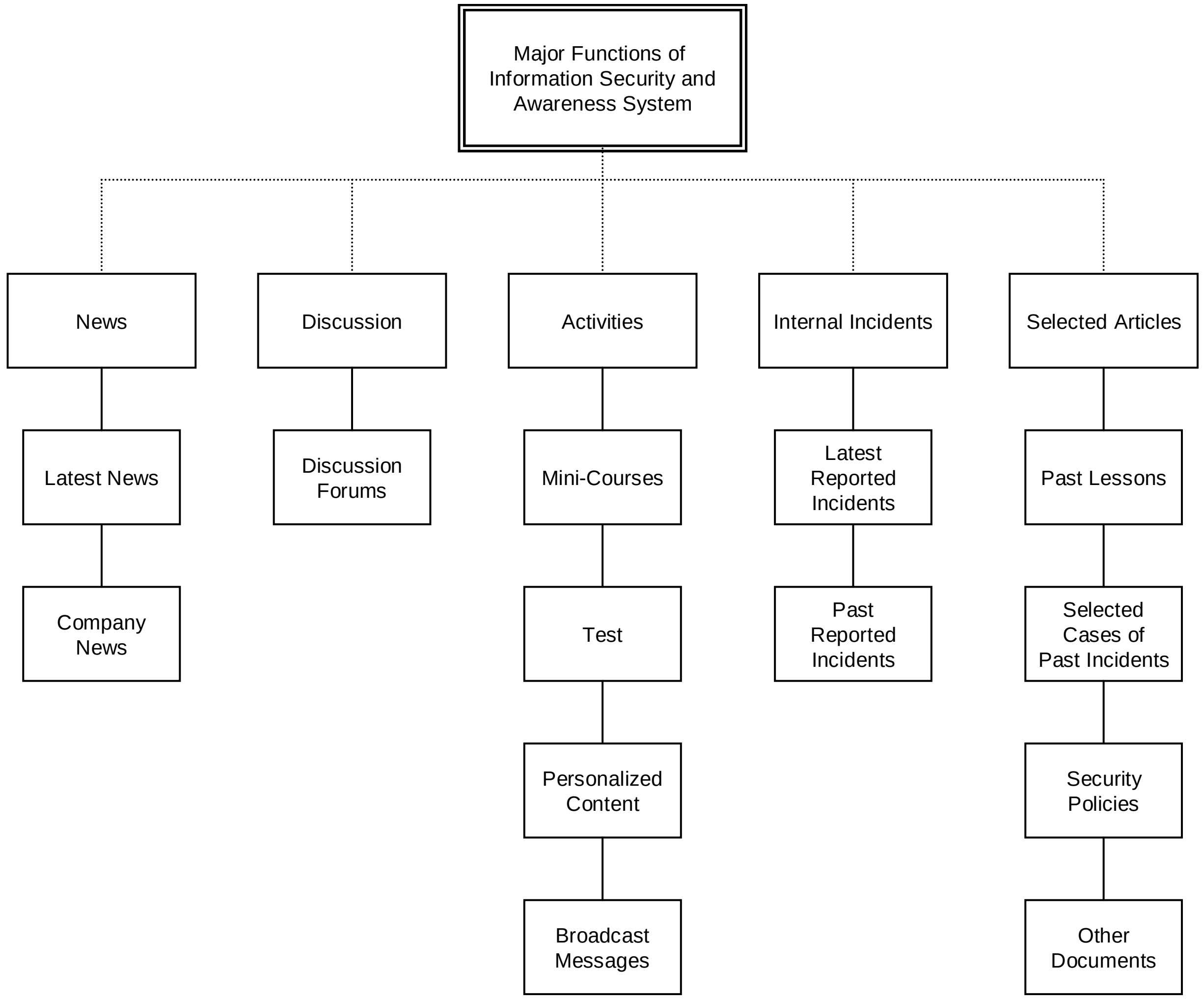
Evaluation Management. Using this component, a system manager can obtain information such as participation behavior and performance records for each participation activity. For example, a manager may use this component to generate a report of the number of discussion messages posted by each employee. This component can also be used to create grade reports of employees taking self-tests of security awareness concepts. Then the system manager can use the reports as the baseline to measure and analyze the security awareness of employees.

The security awareness and administration architecture is established to support a variety of major system functions, which are described in the next section.

User Functions

Based on the interviews with the two senior managers and one training manager of the risk management department, the company required the pilot system to accomplish two objectives, sharing security awareness experiences via news and discussion forums, and providing an online learning environment to improve the security awareness of employees. To meet these two objectives, we incorporated five major functions in the ISAS. Figure 3 shows the major user functions of the system: news, discussion, awareness activities, reports of internal security incidents, and distribution of selected articles on security awareness. Each major function includes one or more sub-functions. For instance, a discussion forum is a useful function that facilitates intra-company discussions. Selected articles should include past security breach incidents, lessons learned from those incidents, security policies, and other security awareness documents. The pilot of this system was web-based so employees could browse these functions via the corporate intranet or, using a login, via the Internet. Each function is detailed as follows:

Figure 3. User Functions of the System



News. Users can browse corporate news according to their authorization levels. New activities and discussion topics can have hyperlinks connecting to relevant news items. Posted news can also be hyperlinked to documents with detailed descriptions and explanations. The system archives the number of visits and displays this statistic next to the news area. The goal is to keep users current and aware of news and activities related to security awareness topics.

Discussion. Discussion forums are created for information exchange among users regarding different security awareness incidents and activities. Users can see the number of online users participating in each discussion forum. The forum can display statistical information on the number of online users participating and show the viewing history of posted contents in the forum. The system manager has the editing flexibility to add and close discussion forums. Users can read posted messages and voluntarily participate in discussions. All activities in the forum are archived for future reference.

Awareness Activities. This function allows users to partake in different awareness activities. The system organizes awareness activities by user groups. Users can explore detailed information about each announced event by clicking its hyperlink. All information related to this event, for example, entry time, browsed contents, and user's identification information, are recorded during browsing. The awareness activities consist of:

- *Minicourse*. Users can go through minicourses on different security awareness topics. Additionally, users can take online tests and get instant feedback on testing results. The system records the usage history and evaluation results.
- *Personalized course content*. A system manager can customize course content based on the needs of each individual. The system can track usage experiences of users on the web server, and the system manager can use the tracking feature to assess if a user has completed the entire awareness activity package.
- *Test*. Management can use online tests to measure the general security awareness level of users. This is a separate activity from the minicourse.
- *Message broadcasting*. Management can broadcast information to users or user groups routinely or randomly and describe security activities and incidents in text messages.

Corporate Incidents. The system can archive reported security breach incidents in chronological order for employees to learn from past incidents. Users in any organizational unit can report incidents based on their own judgment. The system automatically generates e-mail messages informing the system manager of the addition of new incident reports. The system manager can respond immediately to these incidents upon receiving the e-mail messages. After he or she verifies and reviews the security incident, the reporting process is completed. The system manager then uploads the incident report to the web server and informs users to browse it.

Selective Articles. This is an area where a system manager can place information regarding past security activities, incidents and discussions about threats. The system also stores all lessons learned, security policies, and security guidelines. Users can browse the information at their convenience.

System Building

The pilot system was built using the Microsoft Windows 2000 Server operating system, Microsoft Internet Information Services 5.0 web server, PHP web development language, and MySQL 4.0.13 database. PHP and MySQL 4.0.13 are open source applications that let us quickly build a pilot system and deliver necessary features. The interoperability of MySQL with other database systems allows a system manager to collect and analyze the data for future improvement of the system. We implemented all system and user functions described. At deployment, we preloaded the pilot system with ten pieces of news, three security awareness mini-courses, two security awareness tests, and ten security-related articles.

Table 2 shows a sample browsing history of all users in chronological order. If after viewing the browsing history of all users the system manager wishes to drill down, he or she can generate a report similar to Table 3. Table 3 shows the history of web pages visited by a particular user. Note that the report shown in Table 3 only depicts the general activity level of the user and does not show the specific pages he or she browsed. In this case, the time frame overlapped, indicating that the user visited the ISAS through more than one browser instance simultaneously. To get the specific pages that he or she browsed, the system manager would generate a report similar to that shown in Table 4.

Observation and Evaluation Results

Approximately one week after deploying the pilot ISAS, we conducted formal interviews to solicit feedback on the design and functions of the system. We interviewed the same subjects who participated in the study: two senior managers of the risk management department, one training manager of the risk management department, and two assistant managers of the auditing department. These subjects are also users of the system. In general, the interviews attempted to ascertain whether or not the objectives of the system, sharing security awareness experiences via news and discussion forums, and providing an online learning environment to improve security awareness of employees, had been achieved. The interview format was semistructured in that there were major areas that the interviewer had to cover. Within the major areas the interviewees were encouraged to provide as much open-ended feedback as possible. Specifically, the interviews focused on four separate dimensions: system expectations and benefits, the system interface, system management, and other suggestions that may not have been captured by the first three dimensions.

Table 2. Browsing History of Users

User	Hyperlink Activities	Entry Time
Daury	Minicourse1a	2004-3-23 0:29:24
Daury	Minicourse1b	2004-3-23 0:29:39
Daury	Year 2003 Test	2004-3-25 23:7:38
Daury	Minicourse1c	2004-3-25 23:18:13
Daury	Year 2003 Test	2004-3-29 17:26:7
Emily	Year 2003 Test	2004-3-26 0:18:51

Table 3. History of Web Pages Visited by a Single User

# of visits	# of pages visited	Beginning time of browsing	Ending time of browsing	Browsing duration
1	4	25-03-2004 23:52:56	25-03-2004 23:59:12	0h 6mn 16s
2	3	25-03-2004 23:55:37	25-03-2004 23:59:28	0h 3mn 51s
3	1	25-03-2004 23:58:03	25-03-2004 23:58:04	0h 0mn 1s

In general, feedback indicated that expectations about the system and its benefits were met. The pilot system satisfied the requirements gathered, and awareness activities were sufficient for users to get a feel for the system. When asked about the capability to collect data on usage and awareness activities, the training manager replied that the capability provided is not unlike the standard tools used to track users' Internet browsing history, and a system manager should be well versed in using these tools. One manager did add that although the system can collect complete usage records, an analysis of the records and usage history is ultimately what is important. In addition, both the system functions and management architecture are modular in design, which allows users to easily utilize the functions and managers to administer the system. Some interviewees also pointed out that they liked the fact that certain areas, like discussion forums and activities, can be personalized for each user, and this customization based on individual needs can facilitate the absorption of security awareness information.

In terms of system management and interface, the training manager reported that the system was relatively straightforward to operate and maintain. This may be due to the fact that we

Table 4. Summary of Browsing History by User Steve

Page Visited	Frequency
/html/	4
/html/index.php	3
/html/userinfo.php?uid=4	1

used industry-standard and open-source tools to develop the pilot system, as well as that the system was web-based and could be managed asynchronously. Using a relatively simple web development interface, a system manager could adjust the web page layouts and create new awareness activities. The training manager particularly appreciated the ability to manage rights based on user groups. This way, he did not have to painstakingly go through the entire universe of users to set rights and permissions. By and large, users reported that they learned how to use the system, search for information, and participate in discussions within a short period of time, again due to the fact that the system was web-based. Also, those who used dial-up connections from home indicated that the response time was adequate when connected remotely. This response time was due to the fact that a conscious effort was made to not include bandwidth-intensive graphics. Although the lack of fancy graphics improved system response time, a few users did comment on the "plain" appearance of the interface and suggested that a richer appearance be provided in future modifications.

While the five managers were satisfied in general with the pilot system, it should be noted that the system strictly did not attain the second stated objective of providing an online learning environment to improve security awareness of employees. This was because the pilot system was only tested with the five participants, not the general employee population of the host company. Although it was desirable to have more employees participate in the study, the top management at the case site did not want to take up too much of other employees' time, so in the end, five managers at the subsidiary, who were also users of the pilot system, participated in the study. Consequently, the second objective could be attained without including a larger sample of employees in the study. Results of the user reports gathered from the interviews are summarized in Table 5.

Discussion and Conclusions

In this study, we constructed a pilot ISAS and evaluated the system using the systems development framework proposed by Nunamaker et al. (1991). We first developed an architecture for managing the system, then analyzed and gathered user requirements for the pilot system. Based on the user requirements, we designed the requisite system functions and implemented the system. The pilot ISAS incorporated five major functions: news, discussion, activity, internal incidents report and selected articles. To support these functions, we used a management architecture consisting of five components: system management, user management, incident management, awareness activity management and evaluation management.

After building and deploying the pilot system, we interviewed the users and managers to evaluate the system. Based on these results, several themes emerged which may serve as guidelines for building future security awareness systems:

- An ISAS is meant to reach a broad employee base, some of whom may not be technology-literate and security-conscious. At the same time, it is precisely these less technology-oriented employees that the system is trying to reach. Thus, an ISAS needs to be user-friendly and have forward compatibility. The most common method is to adopt a web-based approach in order to allow users to learn and use the system easily and quickly.
- Managers who are also users suggest the importance of generating routine and standard managerial reports for individual users, as well as user groups. This standard function should be included in all ISAS.

Table 5. Summary of Interviewing Results

Dimension	Themes	Results	
Systems Expectation and Benefit	Completeness of functions	• The system provides enough basic functions: online learning, discussion, and incidents reporting.	• The system has many functions for the convenience of system managers and users.
	Sufficiency of awareness activities	• The system provides four kinds of security awareness activities. This should be enough for now. More features can be added in the future.	• The system provides four ways to participate in security awareness activities. System managers can quickly establish security awareness activities.
	Collection of data on usage and awareness activities	• The system can collect information about usage experience and history. A further analysis of collected data is important.	• The system collects complete usage records. Addition and modification of these records are possible for follow-up analysis.
	Flexibility of system design	• The system uses modular design to enhance the convenience of using and managing the system.	• One can easily manage the system because of the modular design.
	Improvement of user awareness	• The system emphasizes personalized design to allow users to quickly search and find useful information. This personalized design can likely help other users improve their awareness levels. Other factors are also important, such as business policy and support and commitment of senior management.	• The system has an area where users can go through activities and share experience and knowledge. Complemented with other features, this system can be a very useful tool.
System Management	Authentication management	• The system assigns authentication rights (including browsing areas and managerial modules) based on user groups.	• The system is easy to manage by authenticating users based on user groups.
	Areas management	• Managers have the flexibility to adjust the webpage layout of the system.	
	Incidents management	• Managers need to evaluate and control what incident reports are allowed taking into consideration corporate public relations.	
	Awareness activity management	• It's easy to operate the system's interface. System managers can easily create new awareness activities via the activity-building interface.	
	Ease of management	• Managers can manage content anywhere anytime because the system is web-based.	• General users can easily manage and maintain the system.
System Interface	Ease of operation	• Ways to operate the system are straightforward. Most people learn how to use the system and search for information within a short period of time.	• Functions of the system are separated in different areas of a webpage to avoid confusing users.
	Webpage layout	• Webpage layout can be customized to provide system managers flexibility to modify a webpage.	• System managers can improve the flexibility of managing webpage layout.
	Response time	• The system does not have fancy graphics to allow fast response time using the dial-up service (56 Kbps).	• Response time of the system is acceptable to most users. There is room for the improvement of interface design.

During the interviews, some interviewees proposed that the collected data about users and awareness activities should be further analyzed. This may help gain insights into the system and examine the utility of different awareness activities and topics, as well as lay a roadmap for future modifications. A full-scale system needs to add this analysis function. Although standard tools that analyze traffic patterns and browsing patterns do exist and can be used, it is still important for a human analyst to examine the analysis results and recommend actions to improve the system.

In addition, there were other suggestions that were not part of the system but, nevertheless, would be important to a successful deployment of ISAS:

- All interviewees emphasized that management needs to review and evaluate incident reports before they are posted for general consumption because the reputation of the company may be at stake. If management decides not to post certain incidents, it should use other forums to communicate awareness regarding these incidents instead of withholding information completely.
- Relevant business policies, financial commitment, and the support of senior management are critical factors for the success of system implementation. For example, senior managers could require their employees to spend a certain amount of time per week on the ISAS and let employees know that their usage histories are tracked by the system. The CEO could personally use the system to broadcast messages to all employees and comment on certain security incidents or commend an employee for practicing good security hygiene.
- The relative ease of use and the minimal and clear functions of the system are two factors that contributed to the acceptance of the pilot ISAS at the host organization. Thus, barriers to the adoption of the system could be reduced by sequentially adding new features rather than at first overwhelming users with functions and features. In addition, a successful case of deployment could help convince users to adopt the system in other locations and subsidiaries.

The study focused on understanding primary functions and systems components of an ISAS. While the ISAS described here was a pilot system, these findings constitute important lessons for organizations that contemplate building effective information security awareness systems.

References

American Society for Training and Development (ASTD). (2001). *A vision of e-learning for America's workforce: Report of the commission on technology and adult learning*. Retrieved October 25, 2005, from http://www.astd.org/astd/publications/whitepapers/about_whitepapers

Claburn, T. (2005, Januray 17). Machine wars: The battle between good and evil in cyberspace is increasingly fought with automated tools. *InformationWeek*, pp. 54-63.

Chen, C. (2003). A constructivist approach to teaching: Implications in teaching computer networking. *Information Technology, Learning, and Performance Journal*, *21*(2), 17-27.

Dam, K. W., & Lin, H. S. (1996). *Cryptography's role in securing the information society*. Washington D.C.: National Academy Press.

Desman, M. (2003). The ten commandments of information security awareness training. *Information Systems Security*, *11*(6), 39-44.

Endsley, M. R., & Garland, D. J. (Eds.). (2000). *Theoretical underpinnings of situation awareness: A critical review*. Mahwah, NJ: Lawrence Erlbaum Associates.

Folkman, S., Lazarus, R. S., DeLongis, A., & Grune, R. J. (1986).Dynamics of a stressful encounter: Cognitive appraisal, coping, and encounter outcomes. *Journal of Personality and Social Psychology*, *50*(5), 995-100.

Fortune. (2005). *The 2005 global 500 full list*. Retrieved November 4, 2005, from http://www.fortune.com/fortune/global500/fulllist/0,24394,1,00.html

Furnell, S. M., Gennatou, M., & Dowland, P. S. (2002). A prototype tool for information security awareness and training. *Logistics Information Management*, *15*(5/6), 352-357.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2005). *CSI/FBI computer crime* *and security survey*. Retrieved October 11, 2005, from http://www.gocsi.com

Hoffman, D. L., Novak, T. P., & Peralta, M. (1999). Building consumer trust online. *Communications of the ACM*, *42*(4), 80-85.

International Organization for Standardization (ISO). (2005). ISO 17799: Information technology—Security techniques—Code of practice for information security management. Geneva: International Organization for Standardization.

Kast, D., & Rosenzweig, J. (1972). General systems theory: Applications for organization and management. *Academy of Management Journal*, *15*(4), 447-465.

Leach, J. (2003). Improving user security behavior. *Computers & Security*, *22*(8), 685-692.

Leidner, D. E., & Jarvenpaa, S. L. (1995). The use of information technology to enhance management school education: A theoretical view. *MIS Quarterly*, *19*(3), 265-291.

Liu, C., Marchewka, J. T., Lu, J., & Yu. C. (2005). Beyond concern—A privacy-trust-behavioral intention model of electronic commerce. *Information and Management*, *42*(2), 289-304.

Loch, K. D., Carr, H. H., & Warkentin, M. E. (1992). Threats to information systems: Today's reality, yesterday's understanding. *MIS Quarterly*, *16*(2), 173-186.

McAdams, A. C. (2004). Security and risk management: A fundamental business issue. *Information Management Journal*, *38*(4), 36-44.

McCrea, F., Gay, R. K., & Bacon, R. (2000, January). Riding the big wave: A white paper on the B2B e-learning industry. San Francisco: Thomas Weisel Partners LLC.

National Institute of Standards and Technology (NIST). (1998, April). *Information technology training requirements: A role- and performance-based model* (NIST Special Publication 800-16). Washington, D.C.: U.S. Department of Commerce.

New York Stock Exchange (NYSE). (2005). *Listed companies directory*. Retrieved November 4, 2005, from http://www.nyse.com/about/

Nunamaker, J. R., Chen, J. F., & Purdin, T. D. M. (1991). Systems development in information systems research. *Journal of Management Information Systems*, *7*(3), 89-106.

PentaSafe Security Technologies. (2002). *Security awareness index report™: The state of security awareness among organizations worldwide*. Retrieved November 5, 2005, from http://security.ittoolbox.com/pub/AM101502a.pdf

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

Timms, S., Potter, C., & Beard, A. (2004). *Information security breaches survey 2004*. Retrieved October 11, 2005, from http://www.infosec.co.uk/files/DTI_Survey_Report.pdf

United States Secret Service (USSS), Chief Security Officer (CSO) Magazine, & Computer Emergency Response Team (CERT) Coordination Center. (2004, May). *2004 e-crime watch survey*. Retrieved October 13, 2005, from http://www.csoonline.com/releases/ecrimewatch04.pdf

Valenta, A., Therriault, D., Dieter, M., & Mrtek, R. (2001). Identifying student attitudes and learning styles in distance education. *Journal of Asynchronous Learning Networks*, *5*(2), 111-127.

Vijayan, J. (2005). Targeting the enemy within. *ComputerWorld*, *39*(32), 23-27.

Wagner, C. (2004). Wiki: A technology for conversational knowledge management and group collaboration. *Communications of the Association for Information Systems*, *13*, 265-289.

Wilson, M., & Hash, J. (2003, October). *Building an information technology security awareness and training program*. Gaithersburg, MD: National Institute of Standards and Technology (NIST).