This story appeared on Information Management Journal at
http://www.entrepreneur.com/tradejournals/article/print/189486076.html
Nov-Dec, 2008

How to create a security culture in your organization: a recent study reveals the importance of assessment, incident response procedures, and social engineering testing in improving security awareness programs.

by Rotvold, Glenda

Information security has become one of the most important and challenging issues facing today's organizations. With pervasive use of technology and widespread connectedness to the global environment, organizations increasingly have become exposed to numerous and varied threats.

Technical controls can provide substantial protection against many of these threats, but they alone do not provide a comprehensive solution. As Kevin Mitnick notes in his book, The Art of Deception: Controlling the Human Element of Security, these technological methods of protecting information may be effective in their respective ways; however, many losses are not caused by a lack of technology or faulty technology but rather by users of technology and faulty human behavior. It stands to reason then that people not only can be part of the problem, but also they can and should be part of the solution. People must be an integral part of any organization's information security defense system.

Keeping information secure is not only the responsibility of information technology (IT) security professionals, but also the responsibility of all people within the organization. Therefore, all users should be aware not only of what their roles and responsibilities are in protecting information resources, but also of how they can protect information and respond to any potential security threat or issue. Security awareness programs address the need to educate all people in an organization so they can help to effectively protect the organization's information assets. But just how well are organizations doing implementing security awareness programs and training their employees?

Security Awareness Study

There are several well-known studies on the topic, including Ernst & Young's "Global Information Security Survey" and CSI/FBI Computer Crime and Security Survey, both done annually. Many of these studies have targeted chief information officers (CIOs), chief security officers (CSOs), and other top-level security professionals and executives in organizations both in the United States and across the globe.

A key difference between these studies and the author's study that is the subject of this article, "Status of Security Awareness in Organizations: An Analysis of Training and Education, Policies, and Social Engineering Testing," is that rather than targeting CIOs and CSOs, this study targets other individuals involved with management of information in various types and sizes of organizations.

The population studied consisted of business professionals (primarily within the United States) including, but not limited to, records, document, and information managers, MIS professionals, legal administrators, archives, administrators, and educators. The survey, therefore, examines security awareness from a different perspective to determine whether similar results would be achieved. The main question is: Do other levels and types of information management professionals have the same level of understanding of security awareness topics, policies, and procedures within their organizations?

The purpose of the study was to investigate the status of security awareness training, IT-related policies, and the use of social engineering testing in business organizations. (The Official (ISC) (2) Guide to the CISSP Exam defines social engineering as: "Successful or unsuccessful attempts to influence a person(s) into either revealing information or acting in a manner that would result in unauthorized access to, unauthorized use of, or unauthorized disclosure of an information system, a network, or data.")

This broad, comprehensive analysis helps provide an analysis of how other levels and types of users perceive security awareness within organizations.

The statistical analysis can help organizations identify potential gaps in their security awareness program, improve their organization's security awareness program, benchmark progress against other organizations, provide insight into components and characteristics of more formalized security awareness programs, and offer insight into the maturity of organizations' security awareness programs. The ultimate goal is to strengthen the human defense security link that guards an organization's information assets.

Rotvold Survey Results

Security Awareness Training: The majority of survey participants (60 percent) reported that their organizations conduct security awareness training. Of the 60 percent that offer security awareness training, 44.7 percent said training is mandatory, and 72.8 percent said attendance is tracked.

This statistic compares to 73 percent of respondents from organizations required to comply with internal control regulations in the 2005 Ernst & Young study involving executives from more than 50 countries. No significant difference by type of organization, number of employees, or region was found on whether training was conducted or mandated or on whether security awareness training on social engineering was conducted.

When training was conducted, the majority of respondents reported that all personnel attend. The most commonly used methods to deliver training included: face-to-face training sessions, e-mail messages, and online training using web- or intranet-based access. Topics covered most often included policies, acceptable use, password protection, workstation security, confidentiality, viruses, remote access, information sensitivity and classification, and bringing in software from home or inappropriate licensing.

Training sessions were offered primarily once a year, typically conducted by information systems (IS) or security staff and were usually flexible enough to incorporate new issues or needs. Results indicated that training was not typically customized for different organizational groups. However, customizing or personalizing the training to show how it can benefit people in their jobs has been recommended by many security experts as a way to increase the effectiveness of the training and help users incorporate what they have heard.

Although input was frequently based on experiences or incidents (53.4 percent), there was agreement by management on topics, and input was also solicited from end users (41.9 percent). The majority of respondents (72.1 percent) had received security awareness training within the last year.

Policies: Because matrix sampling was used, respondents were assigned random sections to complete after finishing the demographics and training sections. Ninety-one respondents completed the Policies section. Only 3.4 percent reported that their organization had no policies. Of the respondents answering the Policies section, the types of policies with the highest-reported percentage of use were acceptable use, e-mail, password, backup and recovery, anti-virus,

software installation and licensing, disaster recovery, and physical security of sensitive areas (See Table 2).

One of the least-used policies was social engineering. Only 20.5 percent of respondents reported that they have policies regarding social engineering, and only 14.3 percent reported the social engineering policies in use.

When asked who participates in the development of information security policies, IS staff received the highest percentage (60.4 percent), followed by IS security personnel (34.1 percent), department managers (24.2 percent), IS steering committee (17.6 percent), and all employees (6.6 percent). Other individual responses included records managers, internal audit, legal, data custodians committee, IT, and vice president of document management.

A majority of respondents reported that policies are easily available, and almost all reported that the security policies were not too restrictive. A high percentage of respondents (83.3 percent) had read one or more security policies within the last year. The majority also reported reading all of the security policies that apply to themselves.

Compliance: Most respondents reported that they were aware of the con sequences for failing to comply with their organization's security policies (81.7 percent). Most organizations also required employees to sign off or attest to reading policies (62.5 percent) and attending training (62.7 percent).

A substantial percentage of respondents reported that there were penalties or consequences for security breaches, including social engineering (48.8 percent); however, 41.5 percent did not know if there were consequences, and only 9.8 percent reported no consequences. As a percent of total respondents, only 2.3 percent provided incentives and rewards for compliance, 13.8 percent used compliance as a factor in employee evaluation, and 30.8 percent reported penalties for non-compliance.

The top three personal motivators reported for compliance were individual motivation, followed by employee responsibility for information security, and importance placed on information security.

Security Awareness and User Perceptions: Respondents were asked to rate their level of agreement or disagreement with several statements regarding security awareness and its status within their organizations. The scale ranged from "Strongly Disagree = 1" to "Strongly Agree = 5." No significant difference by type of organization, size of organization, or region was found on most of the security awareness and perception variables.

The study found many positive perceptions and beliefs regarding various aspects of information security. A high percentage of RIM professionals view information security as important and view people as an important security component. Many also would like to receive more information security training from their organization (M = 3.69). [Editor's note: M = average].

Good security behavior seemed to be neither recognized nor rewarded, yet many respondents felt they were motivated to follow security guidelines either because of individual motivation and employee responsibility or penalties for noncompliance. This would seem to indicate that information security is viewed as part of everyone's job responsibility, and that rewards should not become a primary motivating factor.

Although respondents seem to know to whom they would report a security breach (M = 3.78), they did not believe that incident response procedures were well understood (M = 2.62).

Although these RIM professionals rated their knowledge of the procedures to report a security breach somewhat higher (M = 3.40), it was still some distance from an "Agree" or "Strongly Agree" rating. A possible reason is that only 48.4 percent have incident reporting policies and

only 38.6 percent of those that offer training cover incidents reporting. Another 40 percent do not have any security awareness training.

It is very possible that incidents may go unreported because users may not understand all the events that could be considered a breach nor dearly understand how and when to report a breach. This can represent a serious concern for organizations, became they cannot take appropriate action until an incident is reported.

Survey respondents generally disagreed with statements that said achievement of security awareness goals is measured or assessed (M = 2.66), effectiveness of overall security awareness program is evaluated or measured (M = 2.74), and there was assessment for continuous improvement of the security awareness or information security program (M = 2.79).

Assessment and evaluation are necessary to determine if progress or improvement in security awareness is being achieved, to provide feedback to make adjustments in the program, and to provide a baseline from which to evaluate the program. It is difficult for organizations to improve or even know whether their security awareness training and programs are effective if they do not measure it.

Other areas that potentially could be improved include updating policies on a regular basis, identifying and communicating the security awareness goals and message, repeating the security message often, and creating a security culture.

Creating a Security Culture

Although much progress has been made in improving security awareness in organizations, there is still some work to be done to achieve maturity across the board in these programs. Although 60 percent offered security awareness training, there is still a significant 40 percent that did not.

Organizations that do not have such a program need to look seriously at beginning a security awareness program to strengthen this aspect of their security defense system and protect their information resources. Technology alone is not a comprehensive solution.

Management awareness, commitment, and support were a few of the more common reasons given for security awareness training not being conducted. Involving top management and getting their support is essential in building a strong security awareness program that employees will take seriously. If management commitment is increased, and the security awareness goals and message are communicated and communicated often, progress and improvement can be made in creating a security culture.

Security awareness training needs a foundation of policies. Although many types of policies are in use, there must be more development of polities for incidents reporting, availability/disaster recovery, and social engineering. These policies are extremely important and should be included within an organization's information security program. Once they are developed, it is crucial that employees receive training on these topics.

Assessment of security awareness programs and training is another area that should be examined and strengthened further in organizations in an effort to increase their use so continual improvement and growth can occur. Improvement and growth, in turn, will allow for security awareness to be fully integrated in the organization, assisting in the overall maturing of the information security program.

Security awareness goals first need to be clearly communicated, and the security awareness message repeated often. Assessment is necessary to measure progress in achieving goals and to obtain necessary feedback that can be used to modify and improve the security awareness

program. Assessment also needs to occur periodically so that the program can additionally accommodate the changes and new security issues that arise in such a dynamic environment.

Measurement helps determine whether program and gaining objectives have been met as well as the amount of progress achieved in raising the security awareness of users.

According to Information Systems Audit and Control Association's Security Awareness: Best Practices to Secure Your Enterprise, measurement not only can reveal whether the awareness program is effective, but also can help to identify any knowledge gaps and ensure the continuity and improvement of the overall security awareness program. Surveys, interviews, exams, and audits are a few of the more common assessment tools that can be used to measure progress.

However, social engineering testing is another example of a successful method that can be used to measure the effective ness of an organization's security awareness program. Social engineering attacks against unsuspecting individuals are a type of security threat that can result in significant data loss. Social engineering attacks are increasing. Although these types of attacks can be just as lethal for organizations as other attacks, it is receiving limited attention with organizations. Social engineering polities and training should be developed and implemented.

In this study, social engineering was rated as one of the least-offered training topics in security awareness training, and only half of the 60 percent that offered security awareness training offered social engineering training, Only 20.5 percent of respondents reported social engineering policies, and only 8.1 percent reported social engineering testing. This represents a high level of concern, and efforts should be initiated to ensure policies and training sessions exist on this area.

By implementing some of these changes, organizations can increase coverage of components found in more formalized security awareness programs, achieve higher levels of security awareness maturity, and benefit from a stronger security culture.

Status of Security Awareness in Organizations

In the final analysis, 144 subjects participated in the University of North Dakota research survey conducted by Glenda Rotvold. Participants came from a variety of organizations, including:

* banking (42.%)

* consulting (5.6%)

* education (92%)

* energy and utilities (13.4%)

* financial services (4.2%)

* government (22.2%)

* healthcare (4.2%)

* legal (7.7%)

* manufacturing (8.5%)

* other (20.4%)

The "other" category was used to group participants that did not specify a state, including those from Canada or other international sites.

A majority of the respondents reported that their job duties or responsibilities involved working with IT/information systems security, policies, or user training (82.6 percent). A majority of respondents also classified their job as a management position within the organization (57.6 percent). Table 1. Frequency and Percentages for Security Awareness Training Topics by Percent of Participants in Organizations Reporting Security Awareness Training Offered Security Awareness # Training Topics Respondents % Policies 73 72.3 Acceptable use 73 72.3 Password protection 72 71.3 Workstation security 64 63.4 Confidentiality 62 61.4 Viruses 61 60.4 Remote access 55 54.5 Information sensitivity and classification 52 51.5 Bringing in home software/licensing 50 49.5 Downloading shareware software 47 46.5 Integrity of data/information 40 39.6 Spyware 39 38.6 Incidents reporting 39 38.6 Identity theft 36 35.6 Specialized compliance (HIPAA,FERPA,etc.) 33 32.7 Risk assessment 29 28.7 Availability/Disaster recovery 26 25.7 Social engineering 26 25.7 Service pack or OS updates 17 16.8 Source: "Status of Security Awareness in Organizations: An Analysis of Training and Education, Policies, and Social Engineering Testing" Table 2. Frequency and Percentages for Policies in Use by Percent of Participants in Organizations Completing Policy Section Questions

Security Policies in Use Respondents % Acceptable use 81 89.0 E-mail 77 84.6 Password protection 71 78.0 Backup and recovery 65 71.4 Anti-virus 64 70.3 Software installation and licensing 61 67.0 Ethics 55 60.4 Physical security (sensitive areas) 53 58.2 Disaster recovery 53 58.2 Remote access 52 57.1 Visitor control 52 57.1 Business continuity 45 49.5 Dial-in access policy 38 41.8 E-mail retention 39 42.9 Information sensitivity 44 48.4 Incident reporting 44 48.4 Overall information security plan 37 40.7 IS security plan/program 30 33.0 Patch management 25 27.5 Risk assessment 24 26.4 Vendor oversight 22 24.2 Handheld policy 20 22.0 Extranet 18 19.8 Social engineering 13 14.3 Source: "Status of Security Awareness in Organizations: An Analysis of Training and Education, Policies, and Social Engineering Testing"