Security Awareness Programs

Yu 'Andy' Wu, University of North Texas, USA
Carl S. Guynes, University of North Texas, USA
John Windsor, University of North Texas, USA

ABSTRACT

A critical component of security design is security awareness programs. Implemented effectively, security awareness programs enable organizational members to understand the organization's security posture, their responsibilities, and courses of action in the face of security incidents (Purser, 2004). Awareness training programs should be designed as an initiative to foster organizational learning. In addition to the widely used training methods built with traditional or computer-based media, organizational learning tools, such as cognitive maps, are recommended in training to build security awareness as one type of distributed cognition.

Keywords: Security Awareness; Organizational Learning; Awareness Training; IT security

INTRODUCTION

Security awareness is the processes of making people understand the implications of security on their ability to perform their job. It is important that people understand the importance of security, use of security measures, and reporting processes. Similarly, Boyce and Jennings (2002) suggest that employees should be made aware of security's contributions to the survival, coexistence, and growth of the organization and what is required of them in that respect.

Awareness training programs should be designed as an initiative to foster organizational learning. The training results reside not only in each individual employee but also in organizational memory. With organization memory guiding an employee's sense making and improvisation in case of security incidents, it is more likely that security-smart reactions will become the employee's "second nature." Moreover, to ensure that the employee's behavior is in the best interest for maximizing security, the awareness training should be designed as a systemic system.

Illustrative of the failure of an awareness program is the proverbial user who opens the vicious email attachment. Attachments containing malicious code are one of the oldest and most common tricks for spreading computer viruses. Despite the wide media coverage of their danger, so often users are still opening suspicious attachments that Ernst & Young (2004) uses this as an example to express its concern about lack of security awareness.

SECURITY AWARENESS PROGRAMS

These definitions focus on the cognitive outcomes of awareness training. However, security awareness programs should also aim to generate behavioral outcomes that go beyond the procedural knowledge of using security defense mechanisms. This is because many security breaches result from human negligence and attackers focus on weaknesses in people or processes. Even one single employee's carelessness can undermine the best defense mechanism in place; thus, awareness programs also need to enhance the employee's capability for making sound security judgment and preventing negligence. As Whitman and Mattord (2004) suggest, awareness programs should modify any employee behavior that endangers information security.

Awareness training should be provided to any employee who has contact with the organization's information or information technologies. Their varied degree of contacts with information and IT, however, means that different levels or depths of training are appropriate for different employee groups. Boyce and Jennings (2002)

state that "customization" is often recommended for different types of employees. Alternatively, awareness training can be differentiated based on the specificality of the topic. For example, specific awareness is targeted at specific threats or processes while general awareness covers general topics in security, such as basic security principles (Purser, 2004).

There is a wide spectrum of methods with which awareness training can be delivered. Face-to-face presentation/lecture is one of the most popular. In additional, training materials can be produced with traditional media, such as handbooks, brochures, newsletters, video, etc., or with computer-based media - Web sites, intranet, portals, etc. Some criteria that can be used to evaluate the design of awareness program are continuity, comprehensiveness, coherence, cost-effectiveness, and timeliness (Pipkin, 2000).

ORGANIZATIONAL LEARNING

Templeton defines organizational learning as the set of actions (knowledge acquisition, information distribution, information interpretation, and organizational memory) within the organization that intentionally and unintentionally influence positive organizational change (Templeton, 2002). Similarly, Lee, Courtney, and O'Keefe (1992) subscribe to the view that organizational learning is based on individuals' cyclical interaction processes with their environment. Through the interaction, people derive and update their beliefs about causal-effect relationships. By sharing information on these relationships, they create the knowledge base for organizational learning, which in turn will guide individual as well as organizational action.

Organizations, however, are not a random collection of individuals. Officially, the organization may espouse a *theory of action*, which is formal and normative. However, it is its *theory-in-use* - the theory of action constructed from individuals' actual behaviors that preserve the organization's identity because theory-in-use persists through lapses of time and turnovers in organizational members. It is not static but rather shaped by organizational learning. As agents of organizational learning, individuals continuously restructure the theory-in-use. The encoding of organizational theory-in-use is done by organizational memory, which is where the results of individuals' inquiries are recorded.

INTEGRATION OF ORGANIZATIONAL LEARNING AND SECURITY AWARENESS

Security awareness is an area that may benefit from organizational learning because IT security depends heavily on individuals' acquisition, processing, understanding, and sharing of technology, as well as security-related information, knowledge, and expertise. A conscious effort to learn from past lessons is U.S. Army's Center for Army Lessons Learned (CALL), which is established to institutionalize strategic learning processes into the U.S. army, drawing upon the concepts of organizational learning. It designs an organizational memory system that meets Boland's (1994) principles for IT support of distributed cognition.

The goal of CALL is to induce rapid behavioral transformation in response to changing circumstances (Thomas et al., 2001). The same goal can be set for awareness programs because behavioral changes are what such programs should ultimately achieve and attacks at information systems often create a turbulent or unfamiliar environment. For example, a distributed denial-of-service (DDoS) attack makes an organization's servers incapable of serving customer requests and often creates a public relationship snafu that needs to be handled immediately. Various attacks often cause inexplicable patterns in network traffic, disk activities, etc. For organizational members to cope with such environments, organizational memory can be particularly helpful by enhancing individuals' improvization abilities. In a learned organization, organizational memory is where the emblematic stories are stored. Thus, learning by tapping organization memory enhances individuals' sense-making ability.

Without proper learning, most organizational members lack the background to make sense of tell-tale signs of attacks on information systems. Pertinent knowledge usually resides only in the individual memory of the IT staff. Thus, abnormal system activities may cause a non-IT member, or even IT member, without security expertise, to panic. However, the individual is not able to make sense of it. If the expert member's memory, past security events, and other relevant knowledge are stored in an appropriate format in the organizational memory and shared effectively through organizational learning process, the individual will be able to resort to organizational memory and make sense of the abnormal situation effectively.

DESIGNING SECURITY AWARENESS PROGRAMS

With proper design, an awareness program can encourage the crystallization of an individual's experience, knowledge, and expertise into procedural and declarative organizational memory. Such programs also make the individual aware of the locations in the organizational memory where such procedural and declarative knowledge is stored. Therefore, when individuals encounter suspicious signs in information systems, they will be able to come up with improvisational actions that are more informed, effective, and timely. For example, with training from such programs, individuals, when noticing tell-tale signs of rogue processes on the computer, will be able to tap the organizational memory correctly and efficiently to guide their actions. Not only will they be able to make sense of the signs, but they also will be able to improvise. Depending on the situation, they may decide to record the trace of the processes, actively gather information on the processes, or simply resist the urge to shut down the system so that process information in the computer RAM will not be lost.

The current practice of awareness programs tend to stress customizing training materials to fit an individual or a group of individuals' work environment and daily tasks (Boyce and Jennings, 2002). This is absolutely necessary because it makes the training relevant and interesting to the individual. This personalization often is supplemented with coverage of general security concepts (Purser, 2004). The missing piece of the puzzle, however, is the inclusion of the security implications for other organizational units or members.

Users' behavior can be modified if, even in training specifically customized for non-IT users, materials are included to allow them to stand in the shoes of the IS staff. In addition to pointing out the consequences an unsafe action can cause to the user's work flow, the training program may portray to them the impact such an action will have on the IT staff's work flow. On the other hand, security training of the IT staff tends to focus heavily on the technologies for implementing security defense mechanisms. If "soft" materials are included to create an understanding of what a regular user would feel between a security threat and condescending, jargon-throwing IS "support" staffer, they will become more sympathetic and skillful when helping an individual deal with security breaches.

IMPLICATIONS

In the previous sections, we argued whether IT security awareness programs can be more effective if the designer of awareness training designs the program along the path of organizational learning. Security awareness programs generally come into being out of the necessity to fend off the potential attacks on an organization's information systems. Even when designed with an organizational learning orientation, it is basically a single-loop learning process.

This is not to say, however, that awareness programs shall remain as single-loop learning all the time. A highly effective awareness program may cause the organization to reflect and reevaluate its values if enough updates signify that substantial changes in theory of action are beneficial to the organization's long-term welfare. If organizations choose open source tools for their security defense, awareness programs generally will have to include some exposure to the open source tools and non-Windows platforms such as Linux. Awareness of the alternative tools and platforms may become the first step toward changes in how an organization views and values open source versus Windows software.

When designing the awareness program as an organizational learning system, therefore, particular attention has to be paid to the technological support of organizational learning. Thus, to ensure organizational learning, the designer should focus on the conceptual design of, knowledge representation in, and retrieval and use of organizational memory. For example, if the organization builds a security knowledge base that features hyperlinked fast access and multiple formats of presentation of knowledge, an awareness program can benefit immensely. The superior technical design not only heightens individuals' motivation to explore the knowledge base, but also makes the base a Boland principles-savvy (Boland et al., 1994) component in a distributed cognitive system that facilitates organizational learning.

CONCLUSION

Awareness programs should be designed in such a way that they can leverage organizational memory for employee sense-making and improvisation, hence, their quicker and smarter reactions in cases of security attacks. The key is to encourage active thinking and provide guidance on how to access organizational memory correctly in emergencies. We suggest that IT security awareness programs be designed in a manner that encourages organizational learning. Organizational memory - the core component of organizational learning - can become a repository upon which organizational members can rely to enhance their sense making and improvisational abilities when they encounter suspicious or unfamiliar system activities that may be the result of attacks.

AUTHOR INFORMATION

Dr. Yu "Andy" Wu is an assistant professor in the Department of Information Technology and Decision Sciences, College of Business at the University of North Texas. He received a Ph.D. in Management Information Systems from the University of Central Florida, Orlando, FL, in 2007. His primary research interests include information security and social networks. His research papers appeared in various information systems journals and conferences. Before his academic career, Dr. Wu had experiences administering a corporate network. He has obtained network- and security-related certifications from Cisco, Microsoft, Novell, and CompTIA. E-mail: andy.wu@unt.edu

Dr. Carl S. Guynes is a Regents Professor of Information Systems at the University of North Texas. He received a doctorate in quantitative analysis from Texas Tech University. Dr. Guynes' areas of specialization are client/server computing, end-user computing, data administration, and information resource management. His most recent research efforts have been directed in the areas of client/server computing and data administration. Some of the journals in which Dr. Guynes has published include *Communications of the ACM, Information & Management, The Journal of Information Systems Management, Journal of Accountancy, Journal of Systems Management, The Journal of Database Management, The CPA Journal, The Journal of Computer Information Systems, Information Strategy, Computers and Security, and Computers and Society* . E-mail: Steve.Guynes@unt.edu (Corresponding author)

Dr. John C. Windsor is a professor of Information Systems and former Director of the Information Systems Research Center at the University of North Texas. He received his Ph.D. in Decision Sciences from Georgia State University. He has published six books and over 60 articles in such journals as *Data Base*, *IIE Transactions*, *Information & Management* and *Computers & Security*. His research interests include software and data engineering, systems security, collaborative computing, and the organizational impact of information technology. E-mail: windsor@unt.edu

REFERENCES

1. Boland, R. J., Tenkasi, R. V., & Te'eni, D. (1994). Designing information technology to support distributed cognition. *Organization Science, 5*(3), 456-475.
2. Boyce, J. G., & Jennings, D. W. (2002). *Information Assurance: Managing Organizational IT Security Risks*. Woburn, MA: Butterworth-Heinemann..
3. Ernst & Young LLP. (2004). *Global Information Security Survey 2004*. Chicago, IL.
4. Lee, S., Courtney, J. F., & O'Keefe, R. M. (1992). A system for organizational learning using cognitive maps. *OMEGA, 20*(1), 23-36.
5. Pipkin, D. L. (2000). *Information Security: Protecting the Global Enterprise*. Upper Saddle River, NJ: Prentice Hall PTR.
6. Purser, S. (2004). *A Practical Guide to Managing Information Security*. Boston, MA: Artech House..
7. Templeton, G. F., Lewis, B. R., & Snyder, C. A. (2002). Development of a measure for the organizational learning construct. *Journal of Management Information Systems, 19*(2), 175-218.
8. Thomas, J. B., Sussman, S. W., & Henderson, J. C. (2001). Understanding "strategic learning": Linking organizational learning, knowledge management, and sensemaking. *Organization Science, 12*(3), 331-345..
9. Whitman, M. E., & Mattord, H. J. (2004). Making users mindful of IT security. *Security Management, 48*(11), 32-35.

