End User Security Training for Identification and Access Management

Tonia San Nicolas-Rocca, San Jose State University, San Jose, CA, USA
Lorne Olfman, Center for Information Systems and Technology, Claremont Graduate University, Claremont, CA, USA

ABSTRACT

Identification and access management (I/AM) is among the top security issues facing institutions of higher education. Most institutions of higher education require end users to provide usernames and passwords to gain access to personally identifiable information (PII). This leaves universities vulnerable to unauthorized access and unauthorized disclosure of PII as, according to recent literature, usernames and passwords alone are insufficient for proper authentication of users into information and information systems. This study examines a critical element in the successful implementation of any information security initiative, end user training. Specifically, this study advances research in the area of end user security training by using canonical action research (CAR) to develop and refine an IT security training framework that can guide institutions of higher education in the implementation of USB security tokens for two-factor authentication using public key infrastructure (PKI).

Keywords: Canonical Action Research, Identification & Access Management, Information Technology (IT) Security Training, Knowledge Levels, Public Key Infrastructure

INTRODUCTION

Recent research (Allison et al., 2008; Camp et al., 2007) addresses the need to implement identification and access management (I/AM) solutions within higher education. However, none specifically addresses implementation issues such as awareness and training. A framework that focuses on the implementation of an I/AM solution within higher education for some level of assurance will not only contribute to the field of information systems and technology but will also assist higher education institutions in ensuring some level of I/AM.

Identification and access management, and security have been among the top ten information technology (IT) issues concerning institutions of higher education for the last few years (Ingerman et al., 2010). In the United States, institutions of higher education are both empowered by and dependent on electronic information for academic and administrative...
communications and services (Hawkins, 2007). Most of this information is considered sensitive and, as such, protected by state and federal regulations (which include the Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), the Protection of Pupil Rights Amendment (PPRA), and the Gramm-Leach-Bliley Act (GLBA)) (SanNicolas-Rocca & Olfman, 2009). Unauthorized access into institution computers or network systems and/or unauthorized disclosure of data of any sort can lead to lawsuits, loss of students, bad public relations, termination of employees responsible for unauthorized access, loss of donations, and costs associated with risk assessment and management (SanNicolas-Rocca & Olfman, 2009).

This paper describes the creation and refinement of an IT security training framework at West Coast State University (WCSU) to implement a two-factor authentication system. WCSU was interested in implementing USB eTokens using PKI (public key infrastructure) for two-factor authentication to support federal and state requirements for the protection of PII (personally identifiable information), retention, and preservation of business-critical information, and to ensure I/AM requirements. The IT security training strategy framework was revised and updated by using canonical action research (CAR) with the goal of adapting it for other institutions of higher education, or any other type of organization, for the implementation of an IT security training initiative.

The structure of the paper is as follows. First, we review the literature on identification and access management. We then present the problem situation and describe our canonical action research method. We explain the process of designing the training framework and the implementation of each of the training sessions to the end users. Follow up sessions were provided and subsequent training sessions were refined accordingly. We describe results and modifications to the framework, and discuss limitations, implications and future research directions.

Identification and Access Management

I/AM addresses how and to what degree users employ information as it applies to their role within the organization (Bi, 2008). I/AM processes help initiate, capture, record, and manage user identities, system usage, and security levels, as well as protect proprietary information (Bi, 2008). There are four steps to I/AM: identification, authentication, authorization, and accountability (Harris, 2012). The first three steps (see Table 1) are identification, authentication and authorization (Clark, 2009). The fourth step, accountability, is described by Harris (2012). It applies when authorized access takes place.

Most organizations require users to use a single-factor authentication method to gain access to information and services (Liou & Bhashyam, 2010). This method generally requires the user to provide the correct identifier (e.g., username) in combination with an identity authenticator (e.g., password) that was either user-created or assigned to the user by a system administrator. Unfortunately, even strong passwords are insufficient for proper authentication of users and are considered “weak” as a safeguard in the protection and preservation of PII (Harris, 2012; Smith, 2004).

According to Schneier (2000), “Systems are only as secure as the weakest password”. The security of a system is dependent upon keeping passwords a secret. Unfortunately, there are many ways to divulge passwords. Passwords can be divulged through guessing or finding passwords, giving passwords away, electronic monitoring, an exposed password file, brute force attack, dictionary attacks, social engineering and rainbow tables (Harris, 2012). As a result, many organizations have turned to multi-factor authentication. This process requires users to provide the correct identifier in combination with two or more identity authenticators (e.g., password and a USB eToken).
Sharing Digital Knowledge with End-Users: Case Study of the International Rise Research Institute Library and Documentation Service in the Philippines
www.igi-global.com/chapter/sharing-digital-knowledge-end-users/18196?camid=4v1a