Proposal for Mandatory Information Security Awareness Training
September 19, 2013

Introduction

Leading higher education organizations, information technology and security industries, as well as state and federal agencies have for years promoted awareness training as a critical element to a successful information security program[i]. Most business loss (associated with security breaches) is caused by user error, misconfiguration or mismanagement[ii]. This has been proven to be true at the University of Missouri in that many reported information security incidents are the result of mistakes made by employees.

Current Environment

University employees working in certain areas are already required to complete basic information security awareness training. Those areas include but are not limited to:

- Employees working in health-related fields or organizations and thus, may have access to protected health information (PHI)
- Employees working with personally identifiable financial information. More specifically, employees working in departments that are subject to provisions of the Gramm-Leach-Bliley Act and/or the Federal Trade Commission regulations for protection against identity theft, better known as the identity theft prevention program (ITPP).
- IT staff working for central IT divisions.

There seems to be no single standard or predominant way to organize a security awareness program. Survey results show that these programs within higher education range from voluntary, to initial orientation only, to annual or bi-annual training. One institution surveyed rewards employees for completing awareness training by extending the number of days required for their password reset.

University of Missouri Experiences

Beginning last fall and continuing through early 2013, each of the UM campuses experienced significant disruptions in email services due to successful phishing attacks. The Columbia area users (MU & UM employees) were victimized **183 times by phishing schemes** in FY13. Successful phishing schemes present several serious problems. They place our email systems at risk including the risk of being blacklisted, increase the risk of identity theft, and place other University IT systems and information at risk.

In addition, over the past year and a half, the MU campus information security team responded to a variety of reported incidents. Some of the most concerning categories include:

19	Website defacements
11	Server breaches, server misconfigurations, denial of service attacks or other server-related incidents
12	Protected/confidential information disclosures
15	Acceptable use violation investigations

Combined with the after effects of the previously mentioned phishing schemes, the details of these incidents indicate a general lack of awareness about information security standards and best practices as well as a lack of understanding regarding University information security policies. Both of these problems can be addressed through training.

There is strong support from the CIOs, the UM Chief Information Security Officer (CISO), and the campus Information Security Officers (ISOs) to implement a system-wide information security training program. Additionally, internal audits have repeatedly recommended such training. There are several ways to deliver an effective program. Options include but aren't limited to:

- Annual training for all employees
- Training at new employee orientation with annual or bi-annual refreshers
- More frequent but very brief modules.
- Additional training if/when an employee is known to have caused an incident

Proposal

1. Obtain approval to implement a reoccurring information security awareness training that would be delivered to all University employees.
2. The VP for IT will then develop a program that will provide appropriate training content and deliver such training to all University employees on an annual or bi-annual basis (or some other frequency). Frequency and content will be focused on industry standards as well as known issues and incidents as experienced by the UM campus ISOs.

---

[i] Gartner, SANS, ISACA, Educause, ISC2, FISMA/NIST, OCR, etc.

[ii] *Information Security Awareness Training is Essential to Protect IT Assets*, Gartner, January 15, 2005