Chapter XXXIX
Security Awareness:
Virtual Environments and E-Learning

Edgar Weippl
Vienna University of Technology and Science, Austria & Secure Business, Austria

ABSTRACT

This chapter outlines advanced options for security training. It builds on previous publications (Weippl 2005, 2006) and expands them by including aspects of European-wide cooperation efforts in security awareness. Various examples will show what characterizes successful programs. The authors cooperate with ENISA (http://www.enisa.eu.int/) to create a new multi-language awareness training program that uses virtual environments to allow users to train on real systems without any danger. We describe the design and the proposed implementation of the system. In cooperation with the Austrian Computer Society (http://www.ocg.at) we lay the basis for an ECDL-module on IT security awareness training. Companies are obliged to reasonably secure their IT systems and user awareness training is one of the most important and effective means of increasing security. If claims are filed against a company, it is in the interest of management to provide proof that all users completed IT security training. Moreover, advanced and experienced users need a training environment that lets them try complex scenarios in a safe environment.

INTRODUCTION

The fact that IT security is relevant for companies, universities, and organizations is eventually being picked up by managers, not only by IT professionals. While security often was reduced to the traditional CIA requirements of confidentiality, integrity, and availability, both corporate and non-profit environments also need to take other aspects into account such as validity, completeness, and precision of security policies.

In today’s digital age where we live and work, citizens and businesses find Information Communication Technologies (ICTs) invaluable in daily tasks. At the same time, more and more citizens and businesses are at risk of information security breaches (ENISA 2006).

According to Eurostat, the European Union average (reference period: first quarter for households, January for enterprises) concerning Internet access is that 52 percent of households and 94 percent of enterprises are already connected to the Internet (Eurostat 2006).

It may seem that implementing good security policies can be achieved by reading a couple of good
books and attending one or two training seminars. Clearly, technical personnel such as administrators also need practical training on a technical level. As obvious as this may seem, many companies—especially smaller ones—tend to neglect the training because of daily work. In contrast, large companies usually have established training programs that employees are required to attend.

According to Avizienis (2001, 2004), dependability encompasses five aspects: availability, reliability, safety, integrity, and maintainability. Security is commonly defined as confidentiality, integrity, and availability (CIA).

**Legal Aspects**

It is generally recognized that IT-security is important for almost all companies. Legal requirements such as the Sarbanes-Oxley (SOX) Act on corporate governance have increased awareness at the top executive level to address IT-security among many other issues.

However, small and medium enterprises (SME) typically do not protect their IT assets as well as large companies. In future this will lead to a lower Basel II credit rating and thus make it more difficult for SMEs to remain competitive. The Basel II Accord regulates banks and encourage them to formally calculate their credit, market, and operational risks, including both their IT-security risks and obviously the risks of their clients, too. According to Raschke (2006), “banks in more than 100 countries are expected to implement the Basel II framework beginning in 2008.”

Still, many SME are caught so much in addressing their daily business that they simply do not have the time or the financial resources to properly train their staff.

Their IT infrastructure is often maintained by one or very few employees, usually with limited know-how regarding IT security. Even if SME outsource their IT infrastructure they usually contract small service companies, most of which are not accustomed to even consider using information security standards.

In highly competitive global markets successful SME provide highly customized solutions for their customers. The knowledge of their customers is reflected by the management style. Many SMEs are operated as family businesses. Even though the management usually knows a lot about their customers, they often lack a systematic approach of organizing their business. Such an ad-hoc management style is beneficial to quickly adapt to customer requirements. However, strategic concepts and especially strategic IT security policies are usually not developed. It is clear that ad-hoc security measures are only of limited effect and often overlook important threats and security aspects. Security measures are implemented in the usual ad-hoc way—in most cases after an incident. Several years ago many companies only installed anti-virus software after the company has once been infected.

Lack of knowledge is the main cause for insecure systems (McCoy 2004). Above we have shown that this is especially true for SMEs (Weippl & Klemen 2006). The obvious solution is to train people. However, when designing IT security training we need to take the particular requirements of SMEs into account such as budget constraints and inflexible schedules of IT administration staff.

**Definitions**

- **Availability**—readiness of a system for correct service: Availability is very important for time-critical tasks such as exams. With regard to mass examinations, availability is essential. Apart from unintentional breakdowns of the system, one must not underestimate motivations to knock out the systems on purpose.
- **Reliability**—continuity of correct service: While availability pertains to the system's readiness to perform a service, reliability focuses on delivering a correct service.
- **Safety**—absence of catastrophic consequences on the users and the environment: In most IT-focused companies, safety is no specific issue. While there hazards for human life (fire evacuation of an office building) certainly need to be addressed, they are usually well defined in building codes and regulations of workplace safety.
- **Integrity**—absence of improper system alterations: Integrity in IT systems comprises the integrity of the application and the data. Integrity of the application is necessary to guarantee other requirements such as access control mechanisms to protect the confidentiality and also the integrity of data. Integrity of data is important so that information cannot be modified by unauthorized people.
- **Maintainability**—ability to undergo modifications and repairs: Maintainability refers to the ability of an application to be modified,