Chapter XIX
Information Security Awareness

Gary Hinson
IsecT Ltd, New Zealand

ABSTRACT

This chapter highlights the broad range of factors that are relevant to the design of information security awareness programs, primarily by reference to the literature. It emphasizes the need to supplement technical information security controls with security awareness, training and educational activities to address human vulnerabilities. It outlines requirements noted in standards, laws and regulations, and explains the value of motivational employee communications techniques in creating a security culture.

INTRODUCTION

As with health and safety or legal compliance, management can hardly expect employees to comply with corporate information security policies, adopt security standards and follow security procedures if they don’t even know of their existence. Information security awareness is therefore an essential component of effective information security management systems, supporting and enhancing the technical and procedural information security controls and contributing to the corporation’s overall governance. In order to instill a genuine security culture throughout the organization, the awareness issue goes well beyond simply informing employees of their security obligations. To overcome the inevitable change resistance or inertia, employees have to be both informed and motivated to modify their behaviors, to ‘think security and act securely’. This chapter explains the challenges and details information security awareness approaches that
work, using quotations from others in the field to illustrate the points made.

**BACKGROUND**

**The Importance and Limitations of Information Security**

Information is the lifeblood of organizations, a vital business asset in today’s IT-enabled world. IT systems and networks link every internal department and connect us with a myriad of suppliers, partners and markets. Access to high-quality, complete, accurate and up-to-date information improves managerial decision-making by reducing the margin for error.

Protecting and enhancing the value of information assets has become a central strategic objective in most businesses, second only to making profits. Schmidt (2005) said “We need to build security into the core fabric – the DNA – of the computing world.”

Regulations and laws such as Health Insurance Portability and Accountability Act (HIPAA, 1996), Financial Modernization Act (GLB, 1999), Basel II (2004), Sarbanes Oxley Act (SOX, 2002), Federal Information Security Management Act (FISMA, 2002), and various privacy/data protection laws such as the Data Protection Act (DPA, 1998) impose a raft of obligations.

Information security is not just a simple matter of having usernames and passwords! Information security controls improve the organization’s profitability by reducing both the number and the extent of information security breaches, reducing both the direct and indirect costs (e.g. lost productivity through time lost investigating and resolving breaches and hoaxes; irrecoverable loss of data; expenses incurred in recovering and securing compromised data and systems; notification of customers and regulators; fines for breaching laws and regulations; damaged reputation leading to customer defections and brand devaluation). Furthermore, comprehensive and reliable information security controls reduce the organization’s overall risk profile. Good information security builds management’s confidence and trust, allowing the organization to press ahead with business opportunities (such as eBusiness) that might otherwise be too risky to contemplate. Part of this arises from better knowledge of the extent of security breaches that occur: consistently reporting information about actual and potential (near-miss) security breaches to management is a sign of a mature information security framework.

Despite the self-evident goal of information security, “There is no such thing as security – it is a dream. Security is not an absolute quantity, only a relative commodity,” said Cochrane (1997, p.40). Wang (2005) attributed security failure to three factors:

1. People concentrating too much on security itself;
2. Security measures not aligned with business strategy; and
3. The existence of a communication gap between senior management and IT professionals.

Seeing the ‘big picture’, Wang said, begins with positioning—that is, establishing a security position that suited both company resources and business direction. “It has to be a long-term commitment and sustainable.” Corporate culture is important too, according to Wang. He addressed the problem of the communication gap that exists between senior management and the executives proposing the security measures, saying that the problem lay with ineffective explanation of security objectives. Senior management is often not aware or concerned with the measures.

Menta (2005), commenting on research of the top 350 UK companies listed by the Financial Times, said “Four out of five investors indicated that a significant breach in security would have
Related Content

Fuzzy Quantitative and Semi-Qualitative Risk Assessment in Projects

Engineering Multi-Agent Systems
[www.igi-global.com/chapter/engineering-multi-agent-systems/13471?camid=4v1a](www.igi-global.com/chapter/engineering-multi-agent-systems/13471?camid=4v1a)

An MDA Compliant Approach for Designing Secure Data Warehouses
[www.igi-global.com/chapter/mda-compliant-approach-designing-secure/20678?camid=4v1a](www.igi-global.com/chapter/mda-compliant-approach-designing-secure/20678?camid=4v1a)

Data Mining and Privacy Protection
Armand Faganel and Danijel Bratina (2011). *Surveillance Technologies and Early Warning Systems: Data Mining Applications for Risk Detection* (pp. 31-51).
[www.igi-global.com/chapter/data-mining-privacy-protection/46803?camid=4v1a](www.igi-global.com/chapter/data-mining-privacy-protection/46803?camid=4v1a)