Chapter 8
Information Security in Government

INTRODUCTION

This chapter examines the important issue of the impact of information security in government. Information security is one of the critical issues of Homeland Security Information Systems (HSIS). As we know from Chapter 4, information security is one of the leading concerns of Chief Information Officers (CIO) in the realm of homeland security. This chapter explores the impact of information security on government similarly to a framework provided by Straub and Welke (1998) who believe that the organizational environment, individual characteristics, the information systems environment, and level of threats are related to management perceptions of information security risk. The argument is that the stronger the correlation between changes in these four factors this would have an influence on the perception of management of information security risk. Therefore, the more the organizational culture supports information security the greater the managerial concern. In this chapter there is an argument made that there needs to be more knowledge of the leading issues facing information security in order to influence the organizational culture.

The first part of this chapter focuses on several information security issues that have been identified in the literature. These issues deal with management, policy, and end users of IT and their impact on information security. The second part of this chapter provides evidence from several information security surveys. The last part of this chapter deals with survey results from an information security survey of Texas state agencies.

DOI: 10.4018/978-1-60566-834-5.ch008
INFORMATION SECURITY ISSUES

Seven issues in information security management have been identified in the literature as being important. They are management and information security, organizational culture, information security threats, information security policy, education, deterrence and prevention, and users and information security. Each of these issues are identified and later examined through results from a survey of state government CIOs. The factor that belies all of these issues is having an organizational culture that believes in the importance of information security (Rainey and Steinbauer, 1999).

MANAGEMENT AND INFORMATION SECURITY

With the advancement of IT at a fast pace, it is critical to address the issue of information security in this type of interconnected environment (Chang and Ho, 2006). Chang and Ho argue that management attention to information security has been low compared to other information systems issues. Since IT plays such an integral role in modern governments, information security has to be a key component in modern enterprise planning and management. Survey results indicate that security problems are often caused by the negligence of workers, rather than external attacks. Information security is not just a technical problem; it involves important managerial issues requiring special resources and expertise to address this issue.

Research shows that top management support is a significant predictor of an organization’s security culture and level of policy enforcement (Knapp, Marshall, Rainer, and Ford, 2006). Therefore, for the successful adoption of most IT projects, including information security, top management should support its implementation.

ORGANIZATIONAL CULTURE AND INFORMATION SECURITY

Chang and Lin (2007) believe that technical aspects of information security are managed by people; therefore, the technical solution cannot protect the organization without a good security management policy. Their research shows that enterprises should conduct an integrated strategy combining both information security and organizational culture. Successful information security implementation requires a combination of favorable organizational culture, competent information security technology, and management’s support towards information security. Similarly to top management support, the organizational culture should be supportive of information security for its successful adoption. There should be an emphasis, not just on the technical aspect of information security, but its impact on the organization and its people.

INFORMATION SECURITY POLICY

Whitman (2004) argues that a good information security policy is the number one recommended action an organization can take to safeguard its systems. A good information security policy should outline individual responsibilities, define authorized and unauthorized uses of the systems, provides venues for
Related Content

Understanding Optimal Investment in Cyber Terrorism: A Decision Theoretic Approach
[www.igi-global.com/article/understanding-optimal-investment-cyber-terrorism/64311?camid=4v1a](www.igi-global.com/article/understanding-optimal-investment-cyber-terrorism/64311?camid=4v1a)

Measuring the World: How the Smartphone Industry Impacts Cyber Deterrence Credibility
[www.igi-global.com/article/measuring-the-world/204416?camid=4v1a](www.igi-global.com/article/measuring-the-world/204416?camid=4v1a)

Thoughts for the Future
Andrew Colarik (2006). *Cyber Terrorism: Political and Economic Implications* (pp. 147-165).
[www.igi-global.com/chapter/thoughts-future/7432?camid=4v1a](www.igi-global.com/chapter/thoughts-future/7432?camid=4v1a)

DNS Attacks
[www.igi-global.com/chapter/dns-attacks/25671?camid=4v1a](www.igi-global.com/chapter/dns-attacks/25671?camid=4v1a)