Chapter 7.15
Security Policies and Procedures

Yvette Ghormley
Saint Leo University, USA

ABSTRACT

The number and severity of attacks on computer and information systems in the last two decades has steadily risen and mandates the use of security policies by organizations to protect digital as well as physical assets. Although the adoption and implementation of such policies still falls far short, progress is being made. Issues of management commitment, flexibility, structural informality, training, and compliance are among the obstacles that currently hinder greater and more comprehensive coverage for businesses. As security awareness and security-conscious cultures continue to grow, it is likely that research into better methodologies will increase with concomitant efficiency of security policy creation and implementation. However, attacks are becoming increasingly more sophisticated. While the human element is often the weakest link in security, much can be done to mitigate this problem provided security policies are kept focused and properly disseminated, and training and enforcement are applied.

INTRODUCTION

In the days of mainframes, users were given a username and password, and perhaps an electronic badge to admit them to a computer facility. Those days have long evaporated. With the advent of private broadcast networks, intranets, portable media devices, laptops, and the commercial development of the Internet, security for any kind of business has become a lot more complicated. Moreover, it is costing more. The average loss from unauthorized access to data increased by 488 percent from $51,545 in 2004 to $303,234 in 2005, according to the most recent Computer Security Institute/FBI Computer Crime and Security Survey (McFadden, 2006). For larger companies, recent security breaches were estimated by Ernst and Young to range from $17 to

$28 million per incident (Garg, Curtis, & Halper, 2003), and Austin & Darby (2003) reported that the cost of security breaches to businesses in the USA was $17 billion. Further, correcting the long-term damage, which includes loss of customer confidence, damage to the company's image, and financial consequences, such as stock devaluation for public companies, can be extremely costly, although difficult to estimate. Therefore, developing an effective security policy, implementing it, and ensuring that it is understood and practiced by all employees is essential.

The Approach to Security Policies and Procedures

Companywide policies should be initiated and enforced from the top, and that includes IT security policies. That does not mean to say that technical policies, such as those developed by IT departments, cannot have a specific focus, but the level of technical complexity itself should not be regarded as a barrier that top management can ignore. Tuesday (2002) cites a case study in which an old approved policy was updated at a lower level but ignored by a CEO's assistant, who was essentially acting as the gatekeeper. The eventual result was that the CEO applied for an exception dispensation; however, the antics of the assistant probably caused sufficient disruption that enforcing the updated policy was difficult.

Policies must focus on the most important aspects of security rather than comprise a long list of laundry items in a 200-page manual. For example, one of the most productive ways to review security from scratch is for each business unit to determine what devices and associated data (digital assets) are the most important (Austin & Darby, 2003). From this data, common policies can be formulated, with the establishment of exception procedures for those groups that are not impacted, or who require a different solution.

The creation of simple, nonspecific technology-dependent policies allows for the possibility of change, and flexible approaches. Tomorrow's security problems are not necessarily going to be solved by today's solutions. Both threats and technology change, and policies should be broad enough to accommodate these facts.

Enforcement of policies is also important. Policies can be written and implemented, but if breaches occur, they must be addressed. Not reacting to breaches in policy causes employees to think that a policy can be safely ignored, and increases the risk that real damage will be done the next time an incident occurs.

Last, the roles of individuals in shaping, implementing, and enforcing security policies must be delineated. If responsibilities are not created, there is a tendency for some individuals to assume roles and proceed unilaterally, and others to ignore situations that must be addressed.

This chapter comprises six main sections: (a) methods to determine the constitution of security policies (frameworks, scope, and creation), (b) adoption and implementation of policies into specific procedures, (c) exception procedures, (d) training in security policies, (e) enforcement of security policies, and (f) leadership roles in security policies. Rather than focusing on specific technologies, the intent of the chapter is to create a framework from which security policies and procedures can be derived for any type of business entity. These elements, with emphasis on the constitution of security policies, are discussed in terms of (a) the research that has been conducted, and (b) practical advice that can be utilized.

BACKGROUND

Constitution of Security Policies

Developing Frameworks

Many IS (information security) researchers express skepticism about the use and effectiveness of security policies (Höne & Eloff, 2002), citing