Chapter X
The Social Side of Security

Richard G. Taylor
University of Houston, USA

ABSTRACT

The introduction of new technologies to accumulate large amounts of data has resulted in the need for new methods to secure organizational information. Current information security strategies tend to focus on a technology-based approach to securing information. However, this technology-based approach can leave an organization vulnerable to information security threats. Organizations must realize that information security is not necessarily a technology issue, but rather a social issue. Humans operate, maintain, and use information systems. Their actions, whether intentional or accidental, are the real threat to organizations. Information security strategies must be developed to address the social issue.

INTRODUCTION

The only safe computer is one that is turned off, locked in a safe, and buried 20 feet down in a secret location. (Elsberry, 1999)

Times are a'changing. Long gone are the days when your television only had three channels and a cup of coffee cost 25 cents. Now, satellite and cable services deliver hundreds of channels to your home (and you do not have to go outside in the rain to adjust the antenna). Coffee chains offer five-dollar cups of coffee, which we gladly pay. Perhaps the greatest impact on society in the recent past has been the introduction of new technologies. Vinyl records have been replaced by CDs or digital downloads, our cars can talk to us and give us directions, there are as many computers in homes as televisions, cell phones keep us connected anywhere we go, and the Internet has opened up a world of information and entertainment. I suppose Darwin would refer to this as evolution.

Technology has also entirely changed the landscape in businesses. Computers have become pervasive in the workplace; there is one at every desk. The affordability of data storage allows organizations to accumulate vast amounts of information about their own organization and about their customers. There has been more

digital information amassed in the last 2 years than has been accumulated in the entire history of mankind (O'Rourke, 2005). This plethora of information has been of great use to organizations, allowing them to make more-informed decisions. This wealth of information has also created a new challenge for organizations. They must keep their information secured. Governmental legislation such as HIPAA[1] and GLBA[2] has mandated that organizations protect customer information. Failure to do so can result in large fines and sanctions.

Much as technology has changed the social and business landscape, it has also changed the views of information security. I recall working in the financial services industry in the late 1980s and early 1990s. The focus of information security was keeping the information physically secured by putting locks on doors and file cabinets and having security guards monitor the building. Another concern was the threat from internal employees. Internal fraud could lead to losses, and steps were taken to prevent it. However, in the mid-1990s something happened that changed the entire focus of information security. One single cable was plugged into an organization's network or mainframe, connecting them to the Internet, thus opening up their systems and information to the entire world. This created great concern for managers, as it should have. Organizations started spending significant amounts of money to secure their information from the outsiders who could access their system via the Internet. The focus of information security moved away from implementing procedures to prevent internal fraud and moved to implementing technology measures to keep unwanted intruders out of their systems. Information security was now considered a technology problem.

Though considered a technology problem, organizations must realize that information security is foremost a social and managerial issue. "Information security continues to be ignored by top managers, middle managers, and employees alike. The result of this neglect is that organizational systems are far less secure than they might otherwise be and that security breaches are far more frequent and damaging than is necessary" (Straub & Welke, 1998, p. 442). With the advancements of solutions to address information security issues—firewalls, virus prevention software, biometric identification devices—one has to wonder why organizational information remains vulnerable. This chapter suggests that the primary cause of information vulnerability is that organizations tend to view information security as a technical problem, ignoring the social aspects. This technology-based view has altered the perception of managers regarding information security issues. The result of this current view can be seen in the increasing number of information security incidents.

In 2004, proceeds from information theft were estimated at $105 billion, greater than proceeds from illegal drug sales (Swartz, 2005). The trend has continued in 2005, with millions of people becoming victims of ID theft as a result of poor security. The Internet has become one of the primary threats to organizational information. In 1988, only six Internet incidents were reported; however, for the year 2003 that number had increased to 137,527 (CERT, 2004). The number of incidents was growing so rapidly, that the CERT[3] institute at Carnegie Mellon stopped tracking occurrences after 2003. These incidents, often publicized in the media, have caused an amplification of managers' fears, thus resulting in the implementation of additional technology-based solutions.

Other reports also show the continued information security problem. According to the annual CSI/FBI Computer Crime and Security Survey (Gordon, Loeb, Lucyshyn, & Richardson, 2005), 56% of the organizations surveyed reported an information security incident within their organizations in the previous 12 months.[4] These incidents included virus attacks, unauthorized access to computer-based systems, fraud, sabo-