An Overview of Threats to Information Security

R. Kelly Rainer, Jr.
Auburn University, USA

INTRODUCTION

Organizations and individuals have many information assets, which are subject to an increasing number of threats. The purpose of this article is to provide (1) an overview of the factors that are increasing the threats to information security and (2) an overview of the threats to information security.

BACKGROUND

Several factors are contributing to today's dangerous threat environment. The first factor is the evolution of the information technology resource from mainframe-only to today's highly complex, interconnected, interdependent, wirelessly networked business environment. This environment exposes organizations and individuals to a world of untrusted networks and potential attackers.

The second factor results from the fact that modern computers and storage devices (e.g., thumb drives) continue to become smaller, faster, cheaper, and more portable, with greater storage capacity. These characteristics make it much easier to steal or lose a computer or storage device that contains huge amounts of sensitive information. Also, far more people are able to afford powerful computers and connect inexpensively to the Internet, thus raising the potential of an attack on information assets.

The third factor is that the computing skills necessary to be a hacker are *decreasing*. The reason is that the Internet contains information and computer programs (called scripts) that users with few skills can download and use to attack any information system connected to the Internet.

The fourth factor is that international organized crime is turning its attention to cybercrime, which are illegal activities taking place over computer networks, particularly the Internet. These crimes can be committed from anywhere in the world, at any time, effectively providing an international safe haven for cybercriminals. Computer-based crimes cause billions of dollars in damages to businesses each year, including the costs to repair information systems, the costs of lost business, and the loss of customer confidence.

The fifth factor is downstream liability. Downstream liability occurs in this manner. If company A's information systems were compromised by a perpetrator and used to attack company B's systems, then company A could be liable for damages to company B. Note that company B is "downstream" from company A in this attack scenario. A downstream liability lawsuit would put company A's security policies and operations on trial. Under tort law, the plaintiff (injured party or company B) would have to prove that the offending company (company A) had a duty to keep its computers secure and failed to do so, as measured against generally accepted standards and practices.

At some point, all companies will have some minimal set of standards that they have to meet when operating information systems that connect to the Internet. The models already exist in the form of regulations and laws (e.g., Gramm-Leach-Bliley Act and the Health Insurance Portability and Accountability Act). Contractual security obligations, particularly *service level agreements* (SLAs), which spell out very specific requirements, might also help establish a security standard. Courts or legislatures could cite typical SLA terms, such as maintaining up-to-date antivirus software, software patches, and firewalls, in crafting minimum security responsibilities.

A company being sued for downstream liability will have to convince a judge or jury that its security measures were reasonable. That is, the company must demonstrate that it had practiced due diligence in information security. Due diligence can be defined in part by what your competitors are doing, which defines best practices.

The sixth factor is increased employee use of unmanaged devices, which are devices outside the control of an organization's IT department. These devices include customer computers, business partners' mobile devices, computers in the business centers of hotels, computers in Starbucks and Paneras, and many others.

The final factor is lack of management support. For the entire organization to take security policies and procedures seriously, senior managers must set the tone and provide necessary resources. Ultimately however, lower-level managers may be even more important. These managers are in close contact with employees every day and thus are in a better position to determine whether employees are following security procedures.

THE THREAT ENVIRONMENT

Whitman and Mattord (2003) classified threats into five general categories to enable us to better understand the complexity of the threat problem. Their categories are natural disasters, technical failures, management failures, unintentional acts, and deliberate acts.

Natural disasters include floods, earthquakes, hurricanes, tornados, lightning, and in some cases, fires. In many cases, natural disasters can cause catastrophic loss of systems and data. Technical failures include problems with hardware and software. The most common hardware problem is a crash of a hard disk drive. The most common software problem is errors, called bugs, in computer programs. We discussed management failures in the Introduction.

Unintentional Acts

Unintentional acts are those with no malicious intent and consist of human errors, deviations in the quality of service by service providers, and environmental hazards. Of these three, human errors are by far the most serious threats to information security.

Before we discuss the various types of human error, we categorize organizational employees. The first category consists of regular employees. There are two important points to be made about regular employees. First, the higher the level of employee, the greater the threat the employee might pose to information security. Higher-level employees may have greater access to corporate data and enjoy greater privileges on organizational information systems. Second, employees in two areas of the organization pose significant threats to information security. Human resources employees generally have access to sensitive personal information about all employees. Likewise, information systems employees not only have access to sensitive organizational data, but they often control the means to create, store, transmit, and modify that data.

The second category of employee includes contract labor, consultants, and janitors and guards. Contract labor, such as temporary hires, may be overlooked in information security. However, these employees often have access to the company's network, information systems, and information assets. Consultants, while technically not employees, do work for the company. Depending on the nature of their

Table 1. Human mistakes

Human Mistake	**Description and Examples**
Tailgating	A technique designed to allow the perpetrator to enter restricted areas that are controlled with locks or card entry. The perpetrator follows closely behind a legitimate employee and, when the employee gains entry, asks them to "hold the door."
Shoulder surfing	The perpetrator watches the employee's computer screen over that person's shoulder. This technique is particularly successful in public areas such as airports, commuter trains, and on airplanes.
Carelessness with laptops and portable computing and storage devices	Losing or misplacing them, or using them carelessly, so that malware can be introduced into an organization's network.
Opening questionable e-mails	Opening e-mails from someone unknown, or clicking on links embedded in e-mails (see phishing attacks below).
Careless Internet surfing	Accessing questionable Websites; can result in malware and/or alien software being introduced into the organization's network.
Poor password selection and use	Choosing and using weak passwords (see strong passwords).
Carelessness with one's office	Unlocked desks and filing cabinets when employees go home at night; not logging off the company network when gone from the office for extended period of time.
Carelessness with discarded equipment	Discarding old computer hardware and devices without completely wiping the memory; includes computers, cell phones, Blackberries, and digital copiers and printers.