

• EDITORIAL & COMMENTARY

Friday, February 09, 2007

'Cyber Crime Awareness 101A'

by Robert C. Newman

Biography: Robert C. Newman, CISSP, is an instructor of information systems in Georgia Southern University's Colleges of Business Administration and Information Technology. He may be reached by e-mail at newmanrc@georgiasouthern.edu or 912-486-7563



Robert Newman

In the past, information security was not a major issue within the business community. In today's environment, security lapses can bankrupt a company and destroy a wealth of information. Individuals can lose their life savings and have their credit ratings ruined. Everyone is aware of the attacks that are occurring daily against the information systems used by the nation's businesses.

A number of horror stories have made the computer industry aware that something must be done to quell this threat to computer resources. These threats are taking the form of computer viruses, worms, Trojan horses and scams. Identity-theft announcements are made daily. Because these attacks are being perpetuated over the Internet, the physical controls that were used to protect centralized facilities have become obsolete. New approaches are necessary to protect the public and private assets and resources.

Security Concerns Today

The Internet is plagued with individuals who enjoy the electronic equivalent of creating graffiti on other people's walls with spray paint or causing some type of vandalism to property. Thousands of virus attacks are a recurring menace. Organizations are plagued by denial of service attacks. Many computer and network users are attempting to get real work done over the Internet and have sensitive or proprietary data they must protect. The objective is to keep the undesirables out of the network while accomplishing required activities or tasks.

Two major issues must be addressed when examining network and computer security-accidental and malicious events. An accidental situation can cause as much grief as a destructive attack. It is, therefore, necessary to protect resources from both of these situations. A multitude of methods and procedures are available to address these issues. Various suggestions and alternatives will be presented in subsequent essays.

Industry analysts estimate that in-house security breaches account for a major number of business-computer network attacks. Many of these intrusions may go undetected. A disgruntled employee may seek revenge by deleting or altering files or applications. Another may participate in corporate espionage, given a promise of large rewards. Still another may be looking for insider information for a stock purchase. Others are just inquisitive and try to access forbidden sites and information. Most organizations can successfully discourage insider attacks by assigning specific access rights that provide restrictions to this type of information. Internal attacks can occur because of the knowledge possessed by the personnel who operate on the organization's computer and network systems.

Cybercrimes

Cybercrime encompasses any criminal act dealing with computers and networks (sometimes called hacking). Additionally, cybercrime also includes traditional crimes that are now being conducted through the Internet and the Web. For example, telemarketing and Internet fraud, identity theft, sex crimes and credit card account thefts are considered to be cybercrimes when the illegal activities are committed through the use of a computer and the Internet. Criminals are becoming technically literate, and their activities are more difficult to track because of the worldwide nature of the Internet. Criminal activities can be initiated anywhere in the world using the Internet and other networks.

Criminal activity has increased in the area of networking with the advent of worldwide access to the Internet. This in turn has increased the vulnerability of the computer assets that are accessible through the organization's networks. The U.S. Department of Justice (USDOJ) provides guidance to investigators and prosecutors in the areas of cybercrime and intellectual property matters. This support is provided under the Computer Crime and Intellectual Property Section (CCIPS) umbrella. Many computer crime documents containing computer crime guidance and case studies are available at the Web site www.cybercrime.gov.

There are many categories of cybercrime and security policy issues that must be addressed in today's networking environment. These include identity-theft crimes and various attacks against personal and commercial computer assets. Efforts are underway to identify the vulnerabilities inherent in information systems and devise ways to counter subsequent threats. These activities will be explored in future columns.