BAUER
COLLEGE OF BUSINESS
UNIVERSITY of HOUSTON

ISRC *Notes* – October 2000

Meeting the Security Challenge

Based on a Presentation by Michael Higgins

Protecting information systems from intrusion is a major concern of CIOs and IS managers. The second seminar for the ISRC 2000-2001 year featured a presentation by Michael Higgins, President and Co-founder of Para-Protect Services, Inc., on this topic.

Introduction and Overview

The need for increased connectivity and data sharing in business produces a whole new range of IS-related security problems. While the situation is not as hopeless as described in the media, it is not possible to protect the organizations' data and information systems unless appropriate security measures are implemented. Mr. Higgins subscribes to the Darwinian philosophy; he believes that in managing security, all you have to do is to be "a little bit better than the guy down the street."

Security concerns

Citing different statistics related to computer crime and its impact on business, especially e-commerce, Mr. Higgins emphasized the significance and relevance of the security problem faced by organizations. For instance, in a survey of nearly 1,600 information technology professionals from 50 countries, 73 percent of all companies reported some security breach or corporate espionage during the preceding 12 months (PWC/InformationWeek 1998 Annual Information Security Survey), and $12.5 billion in intellectual property losses were reported in 1998 (IIAP).

The concerns of organizations in the traditional "brick-and mortar" world and the networked world are the same: liability, loss of intellectual property, regulatory violation, embarrassment and reputation loss, loss of market share, extortion, fraud and embezzlement, and systems outage. The major change and concern is that committing these crimes has become easier since the knowledge required for these attacks have become easily accessible. Further, the tools used by the computer criminals are so sophisticated that it is possible to exploit multiple vulnerabilities of the information systems.

People exploit computer-based information systems in different guises for various reasons:

- The "public service" hacker - trying to prove a point
- Hactivists - exposing societal issues
- Script Kiddies - surfing the web & spray painting sites
- Corporate enemies – harming a business
- Disgruntled employees - getting even
- Corporate espionage - Intellectual property (marketing plans, R&D information, manufacturing processes)

Bauer College of Business
University of Houston, Houston, Texas, 77204-6283
Phone: 713-743-4691 Fax: 713-743-4693 E-mail: isrc@uh.edu
URL: http://www.uhisrc.com/

ISRC Information Systems Research Center

When organizations do not apply effective tactics to address security problems, they fail to recognize the threats. In selecting and implementing security solutions, organizations should maintain a business focus. When hiring external consultants to help solve security problems, it is necessary to ensure that the solutions proposed are in line with the business strategy of the organization.

In e-commerce and e-business, the objective of the organization is to deny the competitors market advantage, by maintaining the trust of its customers. To do so, the firm needs to be able to control access to its intellectual property and protect the integrity of the information it presents. Threats that need to be dealt with in the e-commerce environment include increasing number of secondary attacks, viruses to cause malicious denial of service attacks, and multi-source attacks (also referred to as distributed attacks).

Hacking

Four different phases can be identified in the hacking process:

1. *Determine and verify target scope*
2. *Scan and identify vulnerabilities of the target*
3. *Exploit the vulnerabilities of the target*
4. *Cause denial of service or other harm to the target business*

In the first stage, the hacker identifies a target firm for the attack. Firms put a considerable information out on their web sites to satisfy shareholder knowledge and due diligence requirements. Using these and media articles the hacker searches for network links and collects information about all partner and alliance firms of the target firm. Tools and other resources for hacking are available on the Internet and can be easily accessed. Some of these tools were written to help system administrators, while some were written solely to identify and exploit security vulnerabilities.

Different tools like password crackers and commercial network scanning tools are used in the second stage to search for weak passwords and to identify problems in the firm's information systems network. Using these tools, many of which are in the freeware domain, the hacker is able to identify the vulnerabilities of the target firm's information system.

In the third phase, the vulnerabilities are exploited using tools like network sniffer and custom scripts. These tools assist the hacker in stealing passwords and data, installing a trojan for remote access, and removing attack data from system log files and modifying logs. From that point, all it takes is a simple "point & click" to the last stage, in which the hacker can cause damage to the target information systems and consequently, the business.

The discussion on hacking revealed how network technology has made crime easier. Tools and tutorials on hacking and abusing information systems can be easily found on the Internet, and further, can be easily deployed. Though it is possible for Internet Service Providers (ISP) to employ filtering techniques to protect against denial-of-service attacks, they are not willing to do so. Further, the files related to client activities are maintained by these ISP for a very short period that it becomes difficult to track down the source, once an attack occurs. These problems

are compounded by the fact that while computer training is made widely available, commensurate ethics training is not provided.

So, what do you do?

While threats to business due to security problems are real, firms should not panic. It is important to be aware of the problems and be prepared to deal with those. There are two different approaches to managing such risks; one approach is that of risk avoidance, which is costly and ineffective. The other approach is to determine what you are trying to protect and how to protect it. Hence, in developing a plan to solve these problems, firms should:

- Decide what needs to be protected
- How much the protection is worth
- How much loss/compromise/denial of service will cost

Firms should not rush into a solution, because there is no "silver bullet" solution. The solution that you implement does not have to be perfect; any level of protection is good. One option in obtaining security solutions is to seek external expertise; however, it is important to make sure these experts are disinterested and independent of products. In addition, find out what other firms are doing, outside your verticals, as well as inside. When considering bringing in law enforcement agencies to deal with a security issue, firms need to be aware that the business may be disrupted, since the sole focus of these agencies is solving the crime.

There are three aspects to security management: protection, detection, and reaction. The guiding principles in security management are:

- Protect things of value commensurate with the value.
- Detect when things are going wrong.
- React appropriately and expeditiously to detected threats.

Small businesses and home computer users should be aware of the problem of "identity theft." Identity theft is difficult when the user employs a modem connection to access the Internet, but not when a DSL or cable connection is used. Mr. Higgins recommended that users with DSL and cable connections employ a firewall. He recommended two products: blackice.com and nfr.com; both are user-friendly and effective.

Following the presentation, members of the audience discussed some of their concerns with Mr. Higgins. Some of the interesting points are briefly noted below:

- *Governmental agencies often try to provide an environment where research participation for educational institutions is possible; this data sharing compromises the security and protection of the agency's resources. Mr. Higgins commented that organizations should have a legally binding liability agreement for all communication; this is good business practice. Trying to maintain public and private portions of a network is an administrative nightmare. When providing opportunities for data-sharing, security checking via authentication is necessary. Mr. Higgins also noted that having the information out there just because it is technically feasible is not a good enough reason to have it out there.*

- *The threat of IS-based terrorism is real. A transition is occurring in the focus of terrorist activities, moving from threat to Department of Defense centers to civilian services. This will change the way business is done; it can even change the national focus.*

- *The impact of viruses (like the "I love you" virus) is due to the proliferation of a certain operating system. To stop such occurrences, security should become a required feature; customers should demand security. Announcement of security problems should not be cause for discredit for the firm; this will stop firms from providing information about security problems and patches.*
  One of the reasons for outsourcing of security management is that outsourcers can provide quicker upgrades that include security patches.

- *When firms have employees accessing the corporate network from home, a centralized modem security system with smart card interface should be used. Employees should not be using reusable passwords and DSL connections for Internet access. An alternate option for remote access is VPN connection. The technology is available, but ISP do not want to provide that for business reasons.*

- *Very few firms have educational programs about IS security. While 95% of the security measures of a firm are usually focused externally, 80% of threats actually occur from within. Commercially available training videos can be used for training on appropriate use of IS. One recommendation is to use short training videos, with a different version every quarter. Security should be part of every employee's job. Information Technology (IT) staff should be made aware of all vulnerabilities with the system and should be trained to use available technology to fix the problems.*

- *Ensure that agreements between firms do not include uncontrolled access to firm secrets. Make it difficult for the other party to access files they do not need. To avoid straining the relationship, both parties should agree on security measures required to protect their own assets.*