

Electronic Security



Christopher S. Young, Esq.
Business & Technology Law Group
6731 Columbia Gateway Drive
Suite 110
Columbia, Maryland 21046
(410) 290-0707
cyoung@btlg.us

05.20.05

©2005 BTLG

1

Topics:

- What Electronic Security is
- Good news
- Bad news
- Options
- Our invited speaker: B.A. Boit from Sytex

Why is this important to me?

- Increasing network intrusions
- Sophistication level of theft on the rise
- Identity theft on the rise
- Legal obligations related to data

What Is Electronic Security?

False sense of security

Physical security

Some Threats:

- Spamming
- Phishing
- Internet scams (i.e. Nigerian letters)
- Intrusions/Hacking
- Website attacks

Internet Fraud

"Fraud committed via the Internet makes investigation and prosecution difficult because the offender and victim may be located thousands of miles apart. This borderless phenomena is a unique characteristic of Internet crime and is not found with many other types of traditional crime."

----Thomas Richardson, Deputy Assistant Director, Criminal Investigative Division of the FBI.

Possibly the greatest threats:

People behind the firewall: your own employees

The Good News

- Unauthorized access to computer networks is illegal
- Police/FBI and prosecutors are very active in this arena

The Bad News

- Authorities are outpaced by the criminal activity
- Their focus is on terrorism, child pornography and organized crime activities

Corporate Responsibility

For the security of network data

Legal Responsibility

Reasonable efforts to maintain and protect data

What Can I Do About This?

Options:

- Proper network and software foundation
- Hire professionals in the industry
- Conduct regular audits of policies (people are a weak link)
- Update hardware and software
- Backup

Options (Cont'd):

- Employee and company policies (e-mail/data)
- No expectation of privacy on the network
- Home access/home computers

Preventative Measures

The FBI offers the following tips for Internet users:

- If you encounter an unsolicited e-mail that asks you, either directly or through a web site, for personal financial or identity information, such as Social Security number, passwords, or other identifiers, exercise extreme caution.
- If you need to update your information online, use the normal process you've used before, or open a new browser window and type in the website address of the legitimate company's account maintenance page.
- If a website address is unfamiliar, it's probably not real. Only use the address that you have used before, or start at your normal homepage.
- Always report fraudulent or suspicious e-mail to your ISP. Reporting instances of spoof web sites will help get these bogus web sites shut down before they can do any more harm.

Preventative Measures (Cont'd.)

- Most companies require you to log in to a secure site. Look for the lock at the bottom of your browser and "https" in front of the website address.
- Take note of the header address on the web site. Most legitimate sites will have a relatively short internet address that usually depicts the business name followed by ".com," or possibly ".org." Spoof sites are more likely to have an excessively long string of characters in the header, with the legitimate business name somewhere in the string, or possibly not at all.
- If you have any doubts about an e-mail or website, contact the legitimate company directly. Make a copy of the questionable web site's URL address, send it to the legitimate business and ask if the request is legitimate.
- If you've been victimized by a spoofed e-mail or web site, you should contact your local police or sheriff's department, and file a complaint with the FBI's Internet Fraud Complaint Center at www.IFCCFBI.gov.

Resources

- FBI's Internet Fraud Complaint Center (IFCC): <http://www.ic3.gov/>
- Federal Trade Commission ID Theft site: <http://www.consumer.gov/idtheft/index.html>