GSCPA 2011 Annual Convention
Cyber Fraud and Ways to Minimize Your Exposure

Presented by

G. Bliss Jones

gbj@joneskolb.com

June 28, 2011

Cyber Theft Definitions

- **Cyber theft refers to stealing of financial and/or personal information through the use of computers for fraudulent or other illegal use.**
- **Cybercrime, refers to any crime that involves a computer and a network, where the computers may or may not have played a part.**
- **Netcrime refers, more precisely, to criminal exploitation of the Internet.**

Cyber Theft Definitions

Cyber crime can take many forms such as

- **Simple looking into a computer system for which we have no authorization**
- **Creating and distributing a computer virus**
- **Malicious vandalism by a disgruntled employee**
- **Theft of data, money, or sensitive information using a computer system.**

Cyber Theft Definitions

Identify theft is pretending to be someone else in order to gain their assets. The reason for theft is to use another's identity for financial gain. Identity theft has five categories:

1. **Business identity theft,**
2. **Criminal identity theft,**
3. **Financial identity theft,**
4. **Medical identity theft, and**
5. **Identity cloning.**

Cyber Theft: The More Advanced Method of Identity Theft

- **Identity theft can happen to the best of us, even the chairman of the Federal Reserve**
- **An even more sinister form of information theft leading to identity fraud is the stealing of electronic records or stored data (data breaches)**
- **New scanable credit cards are now being read/compromised by scanners in crowds**

Cyber Theft: The More Advanced Method of Identity Theft

- **The Privacy Rights Clearinghouse (PRC), a non-profit consumer advocacy organization, has estimated that well over 500 million electronic records containing sensitive, personal information have gotten into the wrong hands since January of 2005**
- **This number is actually a conservative estimate since they do not count records where they have no idea of the scope of the theft.**

Largest Reported Incidents of ID Theft

130,000,000 2009-01-20 Heartland Payment Systems
94,000,000 2007-01-17 TJX Companies Inc.
90,000,000 1984-06-01 TRW, Sears Roebuck
76,000,000 2009-10-05 National Archives and
40,000,000 2005-06-19 CardSystems, Visa, MC, AMEX
26,500,000 2006-05-22 U.S. Department of Veterans
25,000,000 2007-11-20 HM Revenue and Customs,
17,000,000 2008-10-06 T-Mobile, Deutsche Telekom
12,500,000 2008-03-26 LaSalle Bank, BNY Mellon

Cyber Theft Definitions

Cyber warfare – government sponsored warfare conducted over the internet

McAfee stated in their 2007 annual report that approximately 120 countries have been developing ways to use the Internet as a weapon and target financial markets, government computer systems and utilities.

And If You Do Not Think This is Real

- **A computer virus created to sabotage Iran's nuclear program and stop Tehran developing an atomic bomb is claimed to have been designed by American and Israeli experts.**
- **The Stuxnet computer worm, the most sophisticated cyber weapon ever made, crippled uranium enrichment facilities across Iran last year (2010) and set the country back five years in the nuclear arms race.**

Cyber Theft Definitions

The Federal Bureau of Investigations (FBI) recognizes four instances of cyber crime:

- **National and international Internet fraud**
- **Theft of intellectual property**
- **Publication and intentional dissemination of malware**
- **Cyber crimes against children (usually involving child pornography or child rape)**

And If You Do Not Think This is Real

A group of cyber thieves targeted small-to medium-sized companies, municipalities, churches, and individuals, infecting their computers using a version of the Zeus Botnet. The malware captured passwords, account numbers, and other data used to log into online banking accounts. This scheme resulted in the attempted theft of $220 million, with actual losses of $70 million from victims' bank accounts

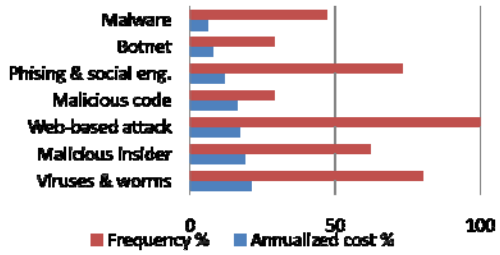
And If You Do Not Think This is Real

"Every corporation is vulnerable to thousands of cyber attacks that occur daily across all industries, causing information theft, disruption to business operations and serious financial loss,"

Dr. Larry Ponemon, founder and chairman of the Ponemon Institute

First Annual Cost of Cyber Crime Study, July 2010

Relative Frequency and Cost of Cyber Crime



America's Ten Most Fraud-Ridden States (per Wall Street Journal 4/4/2011)

Georgia - # 4

- **Population: 9,687,653**
- **Total Complaints: 40,629**
- **Complaints Per 100,000 Population: 419.4**
  - **Georgia has the fourth-highest level of identity theft complaints of all states, with 97.1 complaints for every 100,000 people.**
  - **largest part of these complaints, 31%, dealt with government documents or government benefits fraud**

Phishing, Wire Transfers & Cyber Crime

Phishing, wire transfer and cyber crime is one of the fastest growing and most sophisticated types of fraud that often costs victims tens, if not hundreds, of thousands of dollars in a matter of hours. The increasing scope of this type of fraud has prompted the FDIC, FBI, IRS and AICPA to issue alerts warning about it over the last year.

Phishing, Wire Transfers & Cyber Fraud

How it happens:

1. **Someone opens an innocent looking email and clicks on it to view something. Sometimes you click on a link to take you to another site. It could be a link, an attachment, an unintended web browsing download of a file transfer of a seemingly legitimate/innocent file – see attachment**

Phishing, Wire Transfers & Cyber Fraud

How it happens:

2. **Once you clink on the link, a Trojan horse malware software program is downloaded that tracks your keystrokes and transmits them to a third party while you are on-line.**

Phishing, Wire Transfers & Cyber Fraud

How it happens:

3. **The cyber thief illicitly acquires your login-in credentials and authorization codes to your personal or business on-line banking service with the Trojan horse. The user of the compromised computer is usually unaware that anything malicious has occurred**

Phishing, Wire Transfers & Cyber Fraud

How it happens:

4. **The cyber thief then covertly gains unauthorized access to the victim's computer to avoid bank security features that are activated when the bank does not recognize the login "fingerprint".**

   Effectively the victim's computer is hijacked & used as a trusted source to commit the crime

Phishing, Wire Transfers & Cyber Fraud

How it happens:

5. **Cyber thief takes over your computer and sends out a series of electronic funds transfer (EFT) instructions for amounts just under $10,000 to as many intermediary bank accounts as it can before being detected. Funds are then transferred from the intermediary accounts to foreign accounts almost instantaneously. (There is no float for EFTs.)**

Phishing, Wire Transfers & Cyber Fraud

The aftermath:

- **The primary hope for recovery is that the bank is able to recover the funds by reversing the wire transfers**
- **Funds can be transferred to other non-friendly "havens" in a matter of minutes which minimizes the possibility of recovery/reversal**
- **UCC requires bank notification within two days**

Phishing, Wire Transfers & Cyber Fraud

The aftermath:

UCC Article 4A § 202 says that "a payment order received by the … bank is effective as the order of the customer, whether or not authorized, if … the bank proves that it accepted the payment order in good faith and in compliance with the security procedure and any written agreement or instruction of the customer.

Phishing, Wire Transfers & Cyber Fraud

Risk assessment and minimization:

1. **Conduct a formal risk assessment including the specific activities around the EFT processes**
2. **Can the organization detect an unauthorized wire transfer quickly**
3. **Is the organization in compliance with the bank recommended security procedures**

Phishing, Wire Transfers & Cyber Fraud

Risk assessment and minimization

4. **Does the organization have the type and amount of insurance protection for this type of crime**
   a. **The maximum amount of loss is normally the highest balance in the account where the transfers are handled at any time**

Phishing, Wire Transfers & Cyber Fraud

Risk assessment and minimization:

5. Does the organization have sufficient policies, procedures & controls to avoid this type of fraud.

a. **Proper training and education for employees**
b. **Effective countermeasures for this type of fraud**
c. **Adequate firewalls & intrusion protection software**
d. **What prevents malware from being downloaded**
e. **What prevents computers from being hijacked**

Phishing, Wire Transfers & Cyber Fraud

Specific controls to minimize risk:

- ✓ **Dedicate a computer or system for on-line EFT exclusively (prohibit emails, web browsing, etc.)**
- ✓ **Use multifactor authentication with independent mechanisms such as use of login credentials and a rolling PIN sent to a cell phone or pager**
- ✓ **Log and monitor key computers or systems**

Phishing, Wire Transfers & Cyber Fraud

Specific controls to minimize risk

- ✓ **Segregate EFT controls – one person initiates and a second person approves from a different computer**
- ✓ **Reconcile EFT's daily**
- ✓ **Use a dedicated account with just-in-time deposits**
- ✓ **Use a "run as needed" bootable CD OS (Ubuntu) that cannot be contaminated by a virus (FDIC)**
- ✓ **Turn on o/s & firewall software automatic updates**

The Danger of Using Public Wi-Fi

- **There is a vast increase in the number of computer viruses that are designed in such a way to steal the personal information such as bank account numbers, credit cards data.**
- **The FBI's top cyber-security agent in Chicago warns that when you connect at the corner coffee shop, electronic thieves may be lurking in the air. You shouldn't be checking your personal emails and you definitely shouldn't be checking your personal bank accounts.**