Computer Security Breaches A Threat To Credit Sales

William C. Figg, Dakota State University, USA

ABSTRACT

Business security has progressed from the wooden cash box to the cash register and now the nightmare of the computer. Control has progressively slipped from the control of the instrument operator to a little understood collection of networked instruments. This evolution of difficulty has created numerous protection problems for the business operator. Not only does the cash and other payment means need collection and protection, but now the payment instrument itself has fallen under the responsibility of the vendor. Business owners are as much at risk from cyber security as from physical security. Thieves don't have to rush the store with guns blazing to steal money in fact they don't have to steal money from the store at all. Information and data are the sources of new gold. The information collected from customers' credit cards contains enough data to secure riches for any enterprising evil doer. In addition to normal data growth, regulatory compliance (Sarbanes/Oxley (SOX), SEC17a, HIPAA, Patriot Act, Freedom of Information etc.) is contributing exponentially to data growth, as more records are generated; more regulations are created in more industries. This creates a big fat target as much a target as any "old west" bank, and businesses are responsible for the protection and security of customers' data.

INTRODUCTION

Hackers used to attack computer systems for the fame, more recently; attackers seem to be turning their attention to cybercrime for profit. Cybercrime is a term used to describe criminal activities conducted over the Internet. The most recent Symantec Internet Security Threat Report (2007) found that financial services was the most frequently targeted industry between July 1 and December 31, 2006, making up 84% of phishing attacks. Symantec expects that attacks targeted against the financial services industry will continue to rise as attackers become more profit driven.

Understanding how the attackers are getting into the financial institution's system is the first step in fighting back against the criminals. By understanding how the crimes work, financial institutions can reduce their likelihood of being a victim. Eighty-six percent of the credit and debit cards advertised for sale on underground economy servers known to Symantec were issued by banks in the United States, The Risk of Misreading Generation Y (June 2007).

What methods are attackers using to gain financial information? According to Ted Crooks, vice president of Identity Protection Solutions at Fair Issac, new [internet] scams emerge faster than experts are able to identify and combat (as cited in Bauknight, 2005, p.19). Phishing is a prime example. While a recent increase in stories in the media are educating the general public about it for the first time and are convincing business owners that phishing is a major problem, the attackers are already beginning to move on to more sophisticated and specialized techniques of information theft (Bauknight, 2005, para. 19). Phishing and a similar scam called pharming, are two of the most popular methods for stealing confidential information recently. The best way to fight against these types of attacks is to understand how each one is used to gain access and how widespread the method is used. By learning that information, financial institutions can begin cutting off that access.

According to a study conduced by Time Warner Inc.'s Internet unit AOL and the National Cyber Security Alliance; about one in four U.S. Internet users are targets of phishing attacks and 70% of consumers who were

targeted, believed they were being contacted by a legitimate company (as cited in *PC Magazine Online*, Dec 7, 2005). So what is phishing? The Federal Deposit Insurance Corporation, a federal regulator of financial institutions, defines phishing as a scam that encompasses fraudulently obtaining and using an individual's personal or financial information (Consumer Alerts, May 5, 2005).

In a typical phishing scam, you receive an e-mail supposedly from a company or financial institution you may or may not do business with or from a government agency. The e-mail describes a reason you must "verify" or "resubmit" confidential information – such as bank account and credit card numbers, Social Security numbers, passwords and personal identification numbers (PINs) – using a return e-mail, a form on a linked Web site, or a pop-up message with the name and even the logo of the company or government agency. Perhaps you're told that your bank account information has been lost or stolen or that limits may be imposed on your account unless you provide additional details. If you comply, the thieves hiding behind the seemingly legitimate Web site or e-mail can use the information to make unauthorized withdrawals from your bank account, pay for online purchases using your credit card, or even sell your personal information to other thieves (FDIC Consumer News, Winter 2003/2004).

Identity thieves have even posed as representatives of the Internal Revenue Service (IRS) to try and trick taxpayers into revealing private information that could be used to steal from their financial accounts. Phishing was number three on the list of the 2006 "Dirty Dozen" issued by the IRS in February, 2006. The "Dirty Dozen" is the IRS's annual tally of some of the most notorious tax scams. The Treasury Inspector General for Tax Administration (TIGTA) has reported that it found 12 separate Web sites in 18 different countries hosting variations of the IRS phishing scheme (www.irs.gov, Feb 7, 2006).

Tatiana Platt, AOL's Chief Trust Officer, stated that "Phishers are getting better at tricking consumers into revealing their bank account and financial information, and most Americans can't tell the difference between real e-mails and the growing flood of scams that lead to fraud and identity theft" (as cited by *PC Magazine Online*, Dec 7, 2005). This is a problem for financial institutions for more than the obvious reason of risk to their customers. Phishing has become so widespread, that their customers, who are so fed-up with the daily con attempts, are now unwittingly throwing out the legitimate messages along with the fraudulent ones (Brandt, 2005, p.34).

"You wanted to know who I am, Zero Cool? Well, let me explain the New World Order. Governments and corporations need people like you and me. We are Samurai...the Keyboard Cowboys...and all those other people who have no idea what's going on are the cattle....Moooo." (Hackers 1995)

This is our world now... the world of the electron and the switch, the beauty of the baud. We make use of a service already existing without paying for what could be dirt-cheap if it wasn't run by profiteering gluttons, and you call us criminals. We explore... and you call us criminals. We seek after knowledge... and you call us criminals. We exist without skin color, without nationality, without religious bias... and you call us criminals. You build atomic bombs, you wage wars, you murder, cheat, and lie to us and try to make us believe it's for our own good, yet we're the criminals.
Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for.
I am a hacker, and this is my manifesto. You may stop this individual, but you can't stop us all... after all, we're all alike. (The Mentor, 1986)

Say cybercrime and this is what many people think of, young computer kids breaking into banks and controlling stoplights like they do in the 1995 movie, *Hackers*. The reality is that cybercrime is far more insidious and far reaching than hackers and hacker exploits.

Yes, virus attacks, Trojan horses, and worms are very real threats to computer security, yet the real threat to computer security is often overlooked; the human element. With the ever expanding growth of the Internet and the constantly increasing numbers of users connected to the Internet, there is really no question that cybercrime will continue to increase in the coming years. According to Charlie Fuller (2003), in his book, *Crime and Detection: Cyber Crime*, "Internet traffic increased 25-fold between then [1989] and 1994" (p. 13). By 2002 544.2 million

people were using the Internet, a total of 8.96% of the population. Of course criminals are going to be more and more prevalent as Internet use continues to grow.

Before one can detail cybercrime, how it is perpetrated, how authorities fight it, and how the criminal element continues the cycle by circumventing the enforcement forces, one must define just what cybercrime is.

The *Oxford English Dictionary* defines cybercrime as, "**cybercrime** n.., crime or a crime committed using computers or the Internet." (OED.com, 2006) According to this definition, the perpetration of any crime involving a computer or the Internet is a cybercrime. Technically, this could be considered anything from stealing a computer program to using the Internet to take over the operating account of a Fortune 500 company.

Hackers and hacking are likely the cybercrimes that garner the most media attention. This could be because of the marginalization of the perpetrators or the fact that many of these exploits occur on smaller businesses that do not have the resources to keep the attack quiet and out of the press. There are two types of hackers one has to consider in any discussion of cybercrime.

White hat and black hat. Like the old black and white cowboy movies, the cowboy in the white hat fought for good, while he of the black hat was a villain through and through. White hat hackers do their work to benefit the common good. Curiosity drives these individuals to explore the world of bytes and bits and when, in the midst of their exploits they find an error or weakness, these good hackers inform the author of a software or the network security officer of the network where a weakness was found so that these errors can be repaired to prevent further breaches.

Black hat hackers, as the name implies, are not so benign. They hack for many of the same reasons as their White hat brethren, but their ends are destructive. These hackers find weaknesses in software or network security and exploit these for their own gain. From breaking copyright protection to incrementally siphoning money from bank accounts to their own, these hackers often have the same moral code as your common criminal, they just happen to posses an extensive computer knowledge. And any hacker has to have a well stocked tool box of computer skills. There are a number of 'universal tools' which every hacker, white or black hat seems to posses:

- Knowledge of computer languages such as: C, Java, Perl, C++, and VisualBasic
- General UNIX and/or systems administration knowledge
- Knowledge of network hardware and software
- Security protocol information
- Plenty of spare time (Schell and Martin, 2004, p. 53)

Contrary to the ideas many have about criminal activities, computer criminals are far from being unintelligent thugs, rather they are intelligent people who unfortunately use their knowledge and skills for illegal ends.

These hackers try the patience of policing authorities as they have time and are highly intelligent and seem able to quickly circumvent any new steps the authorities take to block their crimes. The white hat hackers also tend to become the greatest weapon against cybercrime that enforcement agencies have. These hackers turn their natural curiosity and talent against their criminal opposites in an effort to reduce cybercrime.

As soon as the white hat guys and gals come up with a defensive tactic against the blackhats, the criminal element, as in the real world, devise new schemes to get around the enforcement agencies' blocks. Obviously, this aspect of cybercrime becomes a never ending cycle of exploit, defense, and new exploit. Many times these crimes are nothing more than a guy or gal in his or her bedroom or basement just seeing if they can breach some piece of security or copyright, but not always.

It would be nice to say that hackers are the only cybercriminals one would have worry about, but this is not the case. With the proliferation of the Internet and the personal computer, even common, less educated criminals

can harness the power of the web to commit crimes. There seem to be far too many news reports of pedophiles being busted because of their use of computer networks to find under-aged targets. From MySpace to simple Internet searches, pedophiles make use of the power of the computer world to remain anonymous and find victims.

The web makes it so easy for criminals to cover their tracks that it is hard for law enforcement to keep on top of the problem. Unfortunately, the problem is not limited to pimple faced kids hacking in parent's basements and mentally deranged criminals who would commit their crimes with or without the Internet. There are many, many other serious cybercrimes and criminals out there in cyberspace.

Identity theft, a traditional crime, once executed through dumpster diving; the practice of going through garbage looking for things such as social security numbers, account numbers, and other information used to take over another's identity is now aided by the computer and Internet. In a matter of hours, a criminal can completely assume the identity of most anyone on the planet. These criminals divert funds from the mark's bank account to unmarked accounts, secure credit cards in the mark's name, and other exploits to monetarily gain from other's personal information. Because it often takes time for discrepancies to appear on a credit report, many victims do not know they have been affected until a loan application or credit card application has been denied. By this time the criminal's trail is often so cold that it is near impossible to track him or her down.

Apart from being hard to find the perpetrator, identity theft is an expensive crime for the victim to recover from. It takes years for a victim's credit to rebuild fully and it can cost the victim up to or over 10,000 dollars to clean up all the records affected by the thief's activities. In the case of identity theft, the authorities state that the best defense is a good offense. Social security numbers are the key that these criminals need to access the victim's information and steal an identity, so enforcement agencies warn to remove social security numbers from driver's licenses and other identifying documents. As noted on http://www.IDtheftcenter.org, "Guard your Social Security number. When possible, don't carry your Social Security card with you" (Idtheftcenter.org, 2006)

Identity theft is just one traditional crime that has moved to the Internet. Money laundering, "the metaphorical 'cleaning of money' with regards to appearances in law, is the practice of engaging in specific financial transactions in order to conceal the identity, source and/or destination of money and is a main operation of underground economy" is big Internet business (Wikipedia, 2006). The proceeds of money laundering often go to fund the commission of 'real world' crimes such as drug trafficking and terrorist acts. The criminal's use the Internet to route monetary devices through a convoluted path of off shore banks and into different devices such as deposit certificates, bonds, pre-paid credit cards, and gift cards. Through the use of these devices, the criminal is able to wash the illegal source of the money.

To combat this type of cybercrime, the US government has created a number of regulations that US based banks must comply with to help prevent money laundering. However, these steps do not prevent the exclusive use of off-shore banks for money laundering. This adds a dimension of complication when law enforcement is called in to help in a potential money laundering case.

Money laundering, as mentioned above, often leads to terrorist acts, and terrorists are using the Internet in a number of ways to coordinate their activities. As all Americans heard after 9-11, the Internet was a major communicative channel for those involved in the attacks. As of yet, a serious cyber-terrorist attack has not occurred, but the prospect is a chilling one. Since most every aspect of our daily lives connect to computers in some manner, a well devised attack of terrorist funded hackers could literally bring America, and the world to a standstill. Walter Laqueur, an expert on terrorist activity is quoted in the book *Cybercrimes* by Gina DeAngelis as saying, "one U.S. Intelligence official has boasted that, with $1 billion and 20 capable hackers, he could shut down America" (DeAngelis 2000, p. 37).

The best defense against this sort of attack is constant vigilance against the new exploits that hackers use to penetrate networks. By constantly improving and adjusting security measures, the hacker's jobs are made that much harder as the tools in the hacker's bag of tricks are continually made obsolete.

REFERENCES

1. Aftab, Parry. (2000). *The Parent's Guide to Protecting Your Children in Cyberspace.* New York, NY: McGraw-Hill.
2. Authentication in an Internet Banking Environment. (October 2005) Retrieved from Federal Financial Institutions Examination Council on April 5, 2006. Website: www.ffiec.gov.
3. Brandt, A. (October 2005) Phishing anxiety may make you miss messages. *PC World.* 23(10), 34.
4. Bass, Alison. (2001). Defense Against the Dark Arts. *Darwin.* June 2001. Retrieved April 2, 2006 from http://www.darwinmag.com/read/060101/defense.html
5. Bauknight, T.Z. (October-December 2005) The Newest Internet Scams. *Business & Economic Review.* 52(1), 19-21
6. Consumer Alerts – Phishing Scam. (May 5, 2005) Retrieved March 31, 2006, from FDIC: Consumer Alerts – Phishing Scam. Website: http://www.fdic.gov/consumers/consumer/alerts/phishing.html
7. Critics Doubt Effectiveness of California Anti-Phishing Law. (October 5, 2005) *PC Magazine Online*
8. DeAngelis, Gina. (2000). *Cybercrimes.* Philadelphia, PA: Chelsea House Publishers.
9. FDIC Study – "Putting and End to Account-Hijacking Identity Theft" (December 14, 2006) Retrieved from Federal Deposit Insurance Corporation on April 5, 2006. Website: www.FDIC.gov
10. FTC Consumer Alert – How Not to Get Hooked by a 'Phishing' Scam. June 2005. Retrieved from Federal Trade Commission on March 31, 2006. Website: www.ftc.gov/bcp/conline/pubs/alers/phishingalrt.htm
11. Fuller, Charlie. (2003). *Crime and Detection: Cyber Crime.* Broomall, PA: Mason Crest Publishers Inc.
12. Gaudin, Sharon. August 20 2007, "Mobile Workers Think Security is IT's Job"
13. Idtheftcenter.org. (2006). *Prevention Tips.* Retrieved April 2, 2006 from http://www.idtheftcenter.org/preventiontips.shtml.
14. Internet Banking Scams, Cassie Branaugh, April, 2006
15. IRS Announces "Dirty Dozen" Tax Scams for 2006. (February 7, 2006) Retreived March 23, 2006, from Internal Revenue Service. Website: http://www.irs.gov/newsroom/article/0,,id=154293,00.html
16. Kelsey, Nancy & Denise D. Tucker (2005). Former city planner is arrested for having child porn. *Argus Leader.* June 24, 2005. Accessed April 2, 2006.
17. Larkin, E. (November 2005) Spear Phishing. *PC World.* 23(11), 97.
18. Leon, M. (June 6, 2005) The Looming Threat of PHARMING. *InfoWorld.* 27(23), 39-42.
19. McGuire, David. (2004). Report: Kids Pirate Music Freely. *BizReport.* May 19, 2004. Retrieved April 1, 2006 from http://www.bizreport.com/news/7223<a name=/.
20. Mentor, The. (1986). *The Hacker Manifesto*. Retrieved April 2, 2006 from http://www.mithral.com/~beberg/manifesto.html.
21. Mur, Cindy. (2005). *Does the Internet Benefit Society?* Detroit, MI: Greenhaven Press.
22. NBCSandiego.com. (2002). *Police: San Diego Man Kills Girl He Met In Chat Room*. Retrieved April 2, 2006 from http://www.nbcsandiego.com/news/1823797/detail.html.
23. *Oxford English Dictionary* (Online Edition). (2006). Oxford University Press.
24. "Pharming" Guidance on How Financial Institutions Can Protect Against Pharming Atacks. (July 18, 2005) FDIC: Financial Institution Letters. Website: http://www.fdic.gov/news/news/financial/2005/fil6405.html
25. Radcliff, D. (April 11, 2005a) Fighting back against phishing; In the past year, attacks have grown in volume and sophistication, but online merchants are on the offensive with consumer education and new authentication tools. *Network World.* 48.
26. Radcliff, D. (July 18, 2005b) How to prevent pharming; Protect your company's online reputation by locking down DNS and guarding against domain hijacking. *Network World.* 39.
27. RIAA.com. (2006). *What the RIAA is Doing About Piracy.* Retrieved April 2, 2006 from http://www.riaa.com/issues/piracy/riaa.asp.
28. Schell, Bernadette H. & Clemens Martin. (2004). *Cybercrime: A Reference Handbook.* Santa Barbara, CA: ABC Clio.
29. Softley, Iain (Director). (1995). *Hackers* [Motion Picture]. United States: MGM/UA Home Entertainment.
30. Study: One in Four Users are Phishing Targets. (December 7, 2005) *PC Magazine Online.*

31. Symantec Internet Security Threat Report; Trends for July 05 – December 05. (March 2006) IX, Retrieved from Symantec on April 5, 2006. Website: www.symantec.com
32. The Real World of Cybercrime, America Block, April, 2006
33. When Internet Scam Artists Go "Phishing," Don't Take the Bait. (Winter 2003/2004) Retrieved from FDIC: FDIC Consumer News on March 31, 2006. Website: www.fdic.gov/consumers/consumer/news/cnwin0304/phishing.html
34. Wikipedia.com. (2006). *Money Laundering.* Retrieved April 3, 2006 from http://en.wikipedia.org/wiki/Money_laundering.
35. Zell Center for Risk Research, The Risk of Misreading Generation Y, http://www.kellogg.nrthwestern.edu/research/risk/geny/vitalstats.htm June 5, 2007