Radnofsky, M. (2006). “Corporate and Government Computers Hacked by Juveniles.” **The Public Manager** 35(3), pp. 50-55. (full article available at http://www.socratesinstitute.org/research/Hackers.html)

Corporate and Government Computers Hacked by Juveniles

by

Mary L. Radnofsky, Ph.D.
The Socrates Institute

Your government computer is probably being targeted for a hack right now. There’s a good chance the hackers are teenagers. There’s also a good chance they’ll never be caught. And they know it.

Imagine a teenager in his pajamas at the computer in his bedroom at 3 a.m., absorbed by the challenge of hacking into the Pentagon. And then, finally, he comes across a list of thousands of emails from top military brass with cool subjects about different “operations.” There, appearing on the screen before his eyes, are the names and passwords of over a dozen US Department of Defense (DOD) employees. He could be the proverbial fly on the wall at DOD, listening to bio-weapon experts at the Defense Threat Reduction Agency. Yeah, he’ll get to that tomorrow night. OK. Save. And maybe in a week or two, he’ll get to that high-security software for the International Space Station on the National Aeronautic and Space Administration’s (NASA) network. But it’s 4 a.m. and there’s school tomorrow. Bookmark. Shut down.

Seem unlikely? It happened. Yes, this case was “way back” in 1999, when most people hadn’t realized the transparency of computer communication. Except, well, many had. So today in 2006, why are there even more of these cases? Thousands of computer intrusions? Millions of identity thefts? And $67.2 billion lost to cyber-crime last year? The lesson begins two decades ago.

First Hacker Caught - The Germans Learned Their Lesson. But Did We?

The year was 1986. One lone American astronomer, who fiddled with computers during his research, discovered a financial discrepancy of seventy-five cents. From that, he followed a trail of computer hacks over several years, eventually convincing the FBI, military, international security and law enforcement agencies to pursue a computer criminal for the first time in history. In Germany, a college student had gained access to hundreds of computers on Milnet and Arpanet, the US military versions of today's Internet. The hacker downloaded data from our Army bases in Germany, Japan, Alabama, and Georgia, from Air Force bases in Germany and California, from Navy systems in Florida, from the Pentagon, from the Jet Propulsion Lab, from an MIT computer, from the Lawrence Berkeley Lab, and from other defense contractors.

Who *else* had seen the thousands of secret files that a German college student (dubbed the "Hannover Hacker") had been stealing for years? How does one measure the consequences of unveiled defense strategies, proprietary software, and military identities? Perhaps the more recent, though individual, case of Valerie Plame's lost cover can illustrate this point for us today. We won't know how bad things are until something happens based on the lost intelligence. That could be tomorrow or in two months. Hackers are patient, and sometimes wait years before acting on stolen information.

So since 1986, Germans have become the best enforcers of IT security in Europe. Here in the US, however, we are still struggling with postponed legislation (HR 5835), unclear and unevenly enforced laws, and, worst, the battle to convince ourselves that the problem of computer intrusions is in fact a very big deal – not just to industry giants, but to every government agency, school, and home.

The Current State of Cyber-Crime

Twenty years after the Hanover Hacker, we not only still have these types of hacking crimes, but a plethora of even more creative ones, despite the genuine (and expensive) industry and government attempts to secure computer networks. Cyber-crime is, of course, global. Although attacks come from all over the world, twenty-six percent start in the US, followed by China with twenty-four. Many such crimes are committed by students – not because they really want state secrets, but just to prove they can do it. Many more do it for the millions of dollars they can generate through extortion. First they demonstrate they have access, and then threaten to shut down a company's website for a day. So the company pays them *not* to make a denial of service (DoS) hack, and the cyber-criminals get paid time and again.

The most common type of computer crime is "merely" a virus (eighty-four percent of respondents in a 2005 FBI survey said they had experienced at least one), which has high nuisance and economic consequences. But more menacing, and almost as pervasive, are spying incidents (eighty percent also dealt with this). In fact, spyware's legitimate function to help track your child's computer use, for example, makes it freely available on the Internet.

Other problems in cyber-crime include such recently-publicized problems as cyber-stalking, cyber-pornography, child predators, illegal downloading of songs and movies, and software piracy. In addition, a 1999 Rand publication stated that Al Qaeda “appears to have widely adapted information technology,” and was building a terrorist “communications network that relies on the Web, e-mail, and electronic bulletin boards.” Cyber-terrorism was born.

Other examples of cyber-crimes include the following:

- In 2000, a disgruntled worker in Australia hacked into a waste management control system and released millions of gallons of raw sewage into town.

- In 2001, two post-graduate students cracked into a bank system used by the US Treasury Department for Internet transactions, and then generously told the world how they did it.

- In 2003, an 18-year-old who considered himself a gray hat hacker (see sidebar) was arrested for spreading a variant of the “Blaster” Virus, which had infected or shut down millions of computers worldwide. A year later, the Blaster’s original creator was also caught. (Update: spam and junk mail now account for seventy percent of office email, and one in thirty-six such emails contains a virus.

- In 2005, Chinese hackers penetrated US government networks and stole military secrets, including future command and control documents.

- In 2005, the ID theft of 33,000 Air Force officers from a computer at Randolph Air Force Base resulted in the loss of their Social Security numbers, birthdates, and other confidential data. In 2006, the personal information of 26.5 million US veterans and 2.2 million active service members was lost when a laptop with the data was stolen.

- Also in 2006, hundreds of thousands of US and European bankcard numbers and PINS were stolen. Bank accounts were looted, and people lost their life savings. Think Enron losses, and multiply by one hundred.

The Basics of Cyber-Defense – Slow the Flood, Verify Security Measures

So what’s a company or agency to do? Money helps, of course, but despite billions of dollars spent annually on security, there is still an increase in the frequency of computer crimes, many of which may sound like a foreign language to you: There are, as briefly mentioned above, DoS attacks, viruses, malicious code, spying and *key-logging*. In addition, we now have *worms, trojan horses, botnets and zombies, packet-sniffers, war-driving, pharming, spear phishing,* and controlling real-life vital services and utilities such as sewage plants and power grids to entire cities. Yes, hackers can actually disrupt and endanger our personal and professional lives in concrete ways. Phone service can be interrupted; traffic signals can be changed; harassing and threatening emails can be sent in your name.

Let's say, though, that your budget doesn't include billions of dollars for IT (and even if it did, would it want to be constantly on the defensive against computer attacks?). In that case, different solutions are needed, because hackers are persistent. They will "knock at the back door" of your network not just for hours, but for months, or years. Maybe the old software used to keep them out. Double check, though; they may now be in.

So it almost goes without saying that you must install and activate all security hardware and software – and do so correctly. Let's assume you have firewalls and other security on your system. You probably still experience dozens, maybe hundreds of computer intrusions daily, especially spam with viruses or worms. And what about the *bots* or *malcode* that were left behind? Your spam-blocker may have slowed the flood of emails, but it didn't clean out the system. Anti-virus software was installed to run continuously on all employee computers, of course, but it's worth verifying that no one has disabled any of the security measures, which commonly interfere with many programs, and so are frequently "temporarily" disabled. Often, in good faith, the employee intends to re-enable it, but forgets. Other times, it is a conscious choice by dedicated employees to keep it off, because it slows down their productivity. In either case, the damage is done.

Let's also assume, though, that as a dedicated manager, you've sent out positive memos reminding people to follow security procedures. Maybe that's all you've been allowed to do. It's been difficult to enforce cyber-security procedures in the office or with subcontractors, even harder to find leaks, unclear as to how to punish for noncompliance, and vague as to how to deal with actual loss (financial, identity, property). Compliance is still mostly voluntary, with no single government standard uniting them. Until now.

Pending Legislation May Help Enforce Cyber Security Compliance

HR 5835, the Veterans Identity and Credit Security Act of 2006, (proposed following the veterans' ID thefts), has been approved by the House Veterans Affairs Committee as of this writing, and could be signed into law this coming session. The bill, if enacted, would give chief information and security officers the power to enforce cyber-security policies "to the extent determined necessary and explicitly by the head of the agency."

This bill is significant because prior legislation (the 2002 Federal Information Security Management Act, FISMA) was criticized for not having given that power to CIOs, leaving them only able to make cyber-security recommendations. HR 5835 would establish federal standards to notify and provide credit protection services for cyber victims, and enforce instant warnings to Congress or other federal offices impacted by security violations. A controversy now exists as to whether agency undersecretaries or their IT departments should ultimately have IT security enforcement power.

At this point, maybe you're saying that the few intrusions into your network have been fairly innocuous – a few redirected web links to a porn site, or some fake e-mails. But they can escalate in the punch of a key. If someone has the access to send fake emails, they may also be able to read all of yours, and everything else on your hard drive.

Hackers have created an international community that openly shares malicious code, cracker programs, how-to-hack articles, books, workshops, and sites on the Internet and at national conventions. Frequent postings on hacker blogs publicize specific weaknesses in commonly-used applications. Code-specific hacking instructions are accompanied by a disclaimer, "for educational purposes only," but names have been named and weaknesses revealed, making entire networks – government and private –vulnerable to attack.

So even though there is hope that agencies will be able to protect the cyber-infrastructure with new laws or hardware, it may still seem that you have very little control over your own department's computer security. And if you think about the sheer number of human sources as potential data leaks, your control seems even more limited. Cause to worry.

Now, added cause to worry: international cyber-criminals are increasingly linked to organized crime. And as cyber-security software and hardware improve, IBM notes "it is anticipated that many of these criminals may target the most vulnerable access point within a company or organization – *its personnel* – to execute an attack."

In fact, however, and despite the outcome of pending legislation, you actually have as much power with a few well-executed leadership decisions as with your arsenal of cyber-defense measures. There's no physical warehouse to storm, no getaway car to outrun, and no clear-cut bad guy to catch. You have to outwit this enemy, and on his turf. That means education. You have to teach everyone else how to outwit him, too. It all comes back to learning a lesson. Call it training. Call it professional development. Call it continuing ed. Just make sure that the receptionist learns it as does the boss.

Increase Cyber-Security through Education

One agency that has taken an aggressive stance in educating its personnel is DOD, which has developed computer security simulations. They regularly put computer trainees through network attack exercises to learn to thwart actual intrusions.

In fact, the Annual Cyber Defense Exercise (CDX) is the ultimate National Security Agency (NSA) cyber challenge, with the military to educate future officers in the art and science of computer network security. In a simulated military operation, teams of cadets and midshipmen defend a closed computer network they designed, built and configured. Such cyber education is officially acknowledged as essential to this country.

So shouldn't all agencies, businesses and schools be just as dedicated and allocate just as many resources to educating their own communities in the secure, legal, safe, and ethical online practices? The Socrates Institute, a non-profit educational organization founded by this author, certainly thinks so. We began building a cyber-ethics curriculum for schools in 2003, but the problems of cyber-crime had not yet sufficiently caught the public's eye. And since no state department of education required any type of cyber-safety, cyber-security, or cyber-ethics instruction in schools, the federal government did not yet see the need for it either. That's all changing now.

The US Department of Justice (DOJ) Computer Crime and Intellectual Property Section Web site states that "Some individuals exploit the power of the Internet for criminal or terrorist purposes. We can minimize the harm that such individuals do by learning ourselves, and *teaching young people* how to use the Internet safely and responsibly."

The Federal Energy Regulatory Commission (FERC) requires online courses for employees, managers, and technical personnel to "minimize disclosing sensitive information," and *to "teach caution using the web/Internet media.*"

At the state level, Virginia enacted a new Internet Safety Law on March 7, 2006. Merely distributing acceptable use policies has not been effective. The law now has a provision to "include a component on Internet safety for students that is integrated in a division's *instructional* program." In the business sector, Symantec puts its employees through an ethics training program not just once, but yearly and supports Virginia's initiative in protecting children online through classroom instruction. They also add that, "As part of a safety program, the Virginia Department of Education should be looking holistically at Internet safety to *incorporate cyber security and cyber ethics* as well."

Three Aspects of Cyber-Crime Education

These three aspects of cyber-crime education (cyber-safety, cyber-security, and cyber-ethics) form the foundation of the annual C3 Conference at the University of Maryland. The organizer, Dr. Davina Pruitt-Mentle, speaks to its educational focus: "We can use many materials out there in schools, but cyber-ethics, cyber-safety, and cyber-security education won't make an impact until it's *fully integrated* throughout an entire state curriculum. It can't just be an add-on or a school assembly. *It needs to become ingrained into everyone's daily routine*."

Emphatically, The Cyber Security Industry Alliance states that, "What is missing here is a *focused and organized national effort to teach children cyber security, cyber ethics, and cyber safety* with national security in mind." In addition, "it is incomprehensible that we are not teaching cyber security, ethics, and safety at an early age. Poor awareness by children about cyber security may ...ultimately threaten the fabric of our nation's critical cyber infrastructure."

Not surprisingly, one other community also agrees on the importance of cyber crime education. Computer hackers themselves seized the Internet long ago to build a following, create gangs, and challenge each other. As a result, we are dealing today with the somewhat chaotic cyber-culture they built. But as with any culture, this one must evolve in order to survive.

International cooperation in criminal cyber-activity is already underway (the Senate has finally ratified the Council of Europe's 2001 Convention on Cybercrime, making us the sixteenth of forty-three countries to sign). While the treaty sends the signal that we are building a united front to pursue cyber-criminals, it is up to leaders in the cyber-culture to re-establish a united set of values (admittedly an extremely difficult task), and create a common link between what are now tragically disparate nations, at several levels.

Changing Cyber-Culture through Education

Anyone in your office with access to an electronic communication device (from a cell phone to a fax or podcast) risks opening your network to hackers. It doesn't have to be a high-tech piece of equipment either. Information leaks have been happening without laptops for centuries through "Social Engineering." But there are ways to minimize these risks.

So how do employees deal with the cyber-culture in which they work eight hours a day? They make up the rules as they go along. Yes, really. As a result, the cyber-world has as much the freedom, excitement, and danger as the wild-west. But as the Internet reaches a critical mass of users who demand safe, ethical, and secure interactions, it also moves closer to creating a more civilized society.

To facilitate that move, people need to learn *why* they must implement certain security protocols, *why* following one procedure cannot replace all the others, w*hy* certain online activities interfere with security, *why* verifications, back-ups, passwords and firewalls are all needed, etc. Mostly, though, they need to know why *each and every person* should bother with all that even if they are "just" a receptionist or "even though" they're the boss.

It's not enough, of course, to tell people why they should change. To increase the chance of policy being correctly implemented, people need both an understanding of why as well as hands-on training in *how* to change. In computer security, this means letting each employee go through the keystrokes themselves (ideally in a safe, simulated environment) to best understand the importance, relevance, and logic of procedures.

In such simulated environments, we know that learners improve decision-making, make faster choices, apply learned behaviors, and move more easily from novice level to expert. The good news is that simulations can help people learn to avoid Internet credit scams or worms, and to make wise decisions using their own "talents" online. They can learn how to securely instant-message (IM), blog, and use their cell phone without revealing critical information. And throughout the simulation, they will learn the consequences of making wrong decisions.

The bad news is that providing such educational training takes a great deal more time than adding security software, but both strategies are essential to cyber-security.

NetEdGE Cyber-Education

Leaders in both the public and private sectors advocate direct instruction for employees and students in the proper use of cyber-technology. In the spirit of fulfilling this need, The Socrates Institute has been developing NetEdGE (Internet Educational Game of Ethics) with seed money from Symantec. Our purpose is to create a training program that guides young people through different scenarios of cyber-crimes from three perspectives: elite hacker, innocent cyber-victim, and undercover FBI agent. In each role, the individual learns how to interact in a simulated cyber-culture through decision-making, risk-taking, and especially by making mistakes inside the protected environment. We even give players the chance to hack into a fictitious organization, and then have to deal with the legal, economic, and social consequences.

Reaching the current workforce is undeniably important. But we must also reach young people at the start of their career. Nationwide, there are over18.8 million teens on the Internet for an average of ninety minutes a day. Over half (fifty-one percent) of their parents do not have or do not know of software on their computers to monitor where the teens go or with whom they interact online.

But we do know that organized crime has been recruiting teens in great numbers, turning their computer skills into big business. In fact, teens are even recruiting other teens in increasingly organized ways to commit DoS, fraud, and extortion.

We also know that only about five percent of all cyber-criminals are ever caught, and few are punished. In fact, ninety percent of computer intrusions are never even reported; companies prefer not drawing attention to themselves, less they risk losing consumer confidence. So our best chance, and one thing you can do as a leader, to reduce the numbers of cyber-criminals, is to educate the incoming workforce, giving them simulated opportunities to make both right and wrong choice in the cyber-world, and show the real-life consequences of both.

There doesn’t need to be an army of computer hackers to cause damage to an agency infrastructure. All it takes is one young person in a single reckless cyber-crime, and no idea of the social, legal, economic, and emotional damage it can cause. All it takes is one teenager who figures that no one will ever find him. And at three o’clock in the morning, with the world at his fingertips, he’s running password-guessing programs. And he’s not even sleepy.

PostScript

We exist in an unpredictable era of technological evolution that seems to outpace our laws, cultural mores, and sense of personal safety. But we try and keep up with the new cyber-world. So we create new laws. We sit at the same table with security experts and hackers. We invent new strategies to observe it, new tools to probe it, new portals to access it, and new words to define it. Now it's time we developed new ways to teach others (and ourselves) how to successfully, honorably, and safely live in the cyber-world as we do in the real world. The purpose of this article has been neither to recommend nor criticize any particular brand or trademark of computer security; use the system best for your organization, depending on its size, security clearances, or budget. And educate your whole team in how and why to use it – *all* the time.

REFERENCES

Berg, A. January 4,.2006. THREAT MONITOR: "Seven trends to expect from virus and worm authors in 2006." SearchSecurity.com. http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci1155150,00.html

Computer Security Industry Alliance (CSIA). July 2005. Teaching Children Cyber Security and Ethics. White paper.

Department of Justice. 2006. Computer Crime & Intellectual Property Section. http://www.usdoj.gov/criminal/cybercrime/cyberethics.htm#doca

Federal Bureau of Investigation, "2005 Computer Crime Survey Report," 18 January 2006
http://www.mitnicksecurity.com/media/2005%20FBI%20Computer%20Crime%20Survey%20Report.pdf

Hacker Terminology:
• Webster's New World Hacker Dictionary (2006).
• The Jargon File. Glossary of Hacking Terms
http://www.catb.org/jargon/html/go01.html

IBM, January 2006 Global Business Security Index report

http://www-03.ibm.com/industries/financialservices/doc/content/news/pressrelease/1500860103.html

###

Mary L. Radnofsky, PhD is director, The NetEdGE Project and president and CEO of The Socrates Institute. This article has been adapted from a more thorough-going treatment of the topic, including citations for all quotes and references, a glossary of cyber-world terms and other details. For more on NetEdGE or to communicate directly with the author, go to www.socratesinstitute.org.