Cybercrime & Cyberterrorism Against Corporate America

John Hibbs

East Carolina University

Abstract

This paper discusses the methods and techniques used in cybercrime and cyberterrorism in today's society. Cyberterrorism is defined by the Federal Bureau of Investigation as any "premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents."

The discussion topic includes the ideas of cracking, denial of service, unauthorized intrusions, and man-in-the-middle attacks, as well as defenses against these attacks. Possible scenarios that involve these methods of cybercrime and terrorism will be examined including some attack scenarios. After seeing what exactly it is we are facing as a nation with a cyber threat, the next step is to examine how to prevent the threat from happening.

Cybercrime & Cyberterrorism Against Corporate America

In the 1970's the term terrorism might have gotten some consideration but to put cyber with it would have been pure absurdity. Even into the 1980s and the early 1990s, the idea of cyberterrorism would have gotten a professional laughed at. Everything changed in the mid-1990s when the United States government realized the existence of an inevitable fear.

Cyberterrorism is a topic that creates a lot of talk, and a lot of fear. After the events of September 11th the country has experienced a change in how this threat is viewed. Cyberterrorism is essentially defined as: the use of information technology and means by terrorist groups and agents. The threat consists of two fears that are united; the fear of technology and the fear of terrorism. (Krasavin) In the 1990s the United States government began studying this threat. (Armistead, 73)

Many people may associate cybercrime with cyberterrorism, but the two are almost unrelated. Cybercrime is any crime committed over the internet where people are hurt, money is stolen, fraud is committed, or criminals make money. The main motive behind cybercrime is financial gain. Cyberterrorism can be supported by cybercrime, but cybercrime is not necessarily cyberterrorism. (Armistead, 88-89)

As well as having cyberterrorists, people known as hackers, crackers, and hacktivists also exist. Hacking is the unauthorized access to a computer system. Cracking is hacking with criminal intent, and hacktivists are the combination of both hacking and activism.

Hacktivists are politically motivated. They engage primarily in disruptive activities, not destructive. These disruptive actions on the internet usually directly affect

political causes. Such examples may include electronic graffiti on a political web site, denial of service attacks during a politician's campaign, or theft of private information. (Armistead, 82)

Motives of hackers are usually either self accomplishment when defeating the challenge of breaking into a system, to educate themselves of various systems, to find security flaws to assist in the development of patches, or simply to gain recognition of peers. (Armistead, 82)

The events of September 11, 2001 brought much concern to the Bush administration. One of these concerns was that of cyberterrorism. During the aftermath of these traditional terrorist attacks the Bush administration formed the Department of Homeland Security. The purpose of this new governmental department is to: "Create a comprehensive national plan for securing the key resources and critical infrastructure of the United States." The Department of Homeland Security was developed by a combination of five government offices that were merged together. These offices were members of the Federal Bureau of Investigation, the Department of Defense, the Commerce Department, the Department of Energy, and the Federal Computer Incident Response Center. (Armistead, 92)

Some officials, and many private citizens, feel that the threat of cyberterrorism is just an outrageous fear. However, many knowledgeable professionals have testified that this threat is real and could be more dangerous than the traditional means of terrorism. Mr. Walter Laqueur, a well known figure in terrorism studies stated, "The electronic age has now made cyberterrorism possible…". In 1996, well before the events of the September 11th attacks, John Deutch the former director of the Central Intelligence

Agency testified, “International terrorist groups clearly have the capability to attack the information infrastructure of the United States…”. (Armistead, 73)

A third expert, Yonah Alexander, who is a terrorism researcher at the Potomac Institute, stated during a December 2001 announcement the idea of an Iraq net. This supposed network was the compilation of more than one-hundred websites across the globe that was setup by Iraq to perform denial of service attacks against companies with affiliation to the United States. (Weimann)

Following the attacks of 9/11 the government requested $4.5 billion for infrastructure security. The FBI now employs 1,000 cyber investigators to assist with cyber-related issue. (Weimann)

The former director of Homeland Security, Tom Ridge, cautioned that, “Terrorists can sit at one computer connected to one network and can create worldwide havoc.” He also added that, “They don’t need a bomb or explosives to cripple a sector of the economy or shut down a power grid.” (Weimann) As seen by these testimonies the fear of cyberterrorism is real, and should not be over looked.

In addition to numerous forms of attackers, there are numerous forms of “war” that also exists. These include net war, political war, economic war, and cyber war. Net warfare is information-related conflict that is normally against nations with the target being society as a whole. Political warfare has the objective of influencing decisions and policy of leaders of national governments with the primary target being political systems. Economic warfare attempts to influence national government leadership as well, but instead has the target being economic systems. The last form of warfare is cyber warfare.

The goal is to achieve military objectives by conducting war against their targets, with their main targets being military related systems. (Waltz, 17)

There are many types of defenses against all the above mentioned forms of warfare and all forms of hackers, crackers, hacktivists, cybercriminals and terrorists. These range from firewalls to basic virus protection programs to run on the system itself.

The best way to keep your network safe from intruders is a firewall. Firewalls come in many variances. A hardware firewall is physically located between two networks, such as your business network and the internet. A software firewall has the same essential functions as a hardware firewall, except it is a program that runs on each node. The purpose of either firewall is to make all traffic pass through it to be analyzed. Every packet that is passed through the firewall will either receive an explicit deny and not allow access or an explicit permit to allow access. (Waltz, 319)

Traditional firewalls control their traffic by several key functions. The functions included are authentication, packet filtering, application filtering, state and context analysis, and a combination of all the methods working together. Authentication could be as simple as a password and username. Packet filtering looks a little deeper. Every packet that comes into contact is either given the explicit permit or deny based on the firewall rules set in place by the security administrator. Application filtering tends to work like packet filtering in the sense that applications are either allowed or denied based on the rules set in place by what programs can or cannot be allowed. (Waltz, 319)

Another key function to a network is the implementation of a Public Key Infrastructure or a PKI. A PKI keeps a database of public keys stored in a secure area, and every person associated with the network keeps their private key secret. Whenever

an e-mail is sent or comment posted to a forum the employee will sign their document with their private key. When the private key is signed to the document it is then checked against the server with their public key to assure the person that signed the document really is who they claim to be. With this implementation everyone is given the assurance that the person who claims to have written the e-mail is truly who they claim to be. (Waltz, 321-328)

There are also many freely downloadable tools to assist an administrator with his duties of keeping the network secure. Many of these tools can be obtained by visiting the website of insecure.org, who publishes a top list every few years. On the most recent list the top five programs were as follows. Number one is Nessus, which is a UNIX vulnerability assessment tool, Wireshark which is a network traffic sniffer, Snort which is an open source intrusion detection system, Netcat which is available for network debugging, and to finish the top five list was Metasploit Framework, which is an open-source platform for developing, testing, and using exploit code. (Insecure)

Now that the types of attacks have been briefly discussed, as well as a few ways to defend against one, the next important aspects are the phases of an attack. There are five phases to any attack and for the attack to be truly successful all five phases must be properly executed.

During phase one the criminal will do reconnaissance on the victim. Phase two consists of penetration, because until the criminal is inside the system no theft of data or internal disruption can occur. Phase three is executed while in the system to identify and expand their capabilities. Doing damage or stealing information is done during the fourth phase. The final phase is the alteration or removal of evidence, such as deleting log files,

to cover their tracks. An attack that can properly execute the above five phases can create havoc on a system. (Colarik, 83)

With the five phases above there are a few types of attacks that criminals tend to use the most. These include viruses/worms which can create the most havoc for an administrator. Web defacements of sites, commonly referred to as electronic graffiti, is frequently done by hacktivists or just a person attempting to create distraction instead of destruction.

Another dangerous and very costly threat to an organization is that of unauthorized intrusions. Typically a cybercriminal or terrorist will use this type. Once inside a system the intruder is free to do as they please until someone stops them, which may be too late.

Denial of service and distributed denial of service attacks are also very common as they keep the host tied up with their attack and is unable to assist any other user and therefore keeps the user from using the resources stored on the host.

An attack that occurred in 2002 consisted of alteration of Domain Name Service servers. In this attack all thirteen root DNS servers were subjects of a distributed denial of service attack for one hour. Eight of the thirteen servers were disabled, resulting in no noticeable service disruption, only because support servers rarely need to contact the root servers. However, if the attack would've succeeded then no end user would be able to use the internet until the attack was stopped. (Waltz, 55)

To continue with the idea of cyberterrorism there are many attack scenarios that cause fear in officials. There are a few appealing characteristics to terrorists of cyberterrorism compared to traditional forms. These characteristics include the fact that

a cyber attack is cheaper, more anonymous, it can be conducted remotely, and the attack has the capability of affecting a larger number of people. (Weimann)

Over the past few years the FBI has identified numerous cyber threats ranging from simple defacements of web sites to sophisticated intrusions possibly originating in a foreign country. With this new fear of threats the FBI, in January 2002, sent a message regarding the possible attempts by terrorists to use United States municipal and state web sites to obtain information on local energy infrastructures, water reservoirs, dams, highly enriched uranium storage sites, and nuclear and gas facilities. This threat alone is severe enough to affect the entire population for which that particular function serves. The entire attack could be done from another country, by a completely unknown and anonymous enemy, who may never be caught and brought to justice. (Watson)

In the Riptech Internet and Security Report Volume II, it noted the Power and Energy, Financial Services, and High Tech sectors as having higher attack activity while E-commerce and Manufacturing were victims from moderate to low rates. After the attacks of 9/11 in quarters three and four of 2001 the Power and Energy Sector companies suffered a severe attack 57% of the time. In quarters one and two of 2002 the attacks rose to 70% of the time. (Colarik, 118-119) With a terrorist being capable of hacking into a power grid system, then they have the capability of shutting down power to an entire region in the United States. Without power a region is vulnerable to anything, and possibly setting up a larger more traditional attack.

The September 2003 edition of Symantec's Internet Security Threat Report showed the top ten cyber attack countries were as follows: Peru, Iran, Kuwait, United-Arab Emirates, Nigeria, Saudi Arabia, Croatia, Vietnam, Egypt, and Romania. With a

very high probability that at least one of these countries has residents who do not like the United States then with ample time and patience a severe attack could come from any one of these countries, and be virtually impossible to track if properly executed.

Numerous citizens around the world have been victims of identity theft or have had money stolen from personal or business bank accounts in usually the thousands of dollars of loss. The 2003 Encyclopedia of Global Industries reported that the ten largest banks had over $7.5 trillion in United States assets. (Colarik, 124) The ability to hack into these ten banks and steal just a one-hundredth of the total amount will result in the wire transfer of billions of dollars that may never be recovered.

In 2004 the United States Census Bureau reported United States healthcare expenditures totaled $1.6 trillion. An attack to disrupt healthcare could prove to be detrimental to American citizens with this amount of money at stake. Even with monetary values aside an intrusion could modify or steal confidential medical files. With modification to medical records the outcome could cause a physician to prescribe the wrong medicine or course of treatments for their patient with the worst case scenario ending with death. For theft of data for example, a criminal might hack the Center for Disease Control's database and publish to the internet a list of everyone with a status of HIV positive which would result in the public embarrassment of many Americans. (Colarik, 131)

With all the fear raised by cyberterrorism and cybercrime there are a few possible solutions to help lower the risk of the situation but not eliminate the risk. The first solution would be to organize a Global Information Center. This Global Information Center would have the job function of storing all data relevant to risks, to record all

information related to attacks against an organization, manage a threat database, and to investigate where the attacks originated from. The idea of this would be the same as the idea behind the SANS Institute and CERT Coordination Center, but working globally and not just regionally. (Colarik)

Another program to assist in the nation's security would be the implementation of Law Enforcement Tiger Teams. A tiger team is a military term that describes a group of penetration specialists that conducted security reviews of friendly installations. During and after an attack this team would be contacted. Whenever an attack is happening in real-time their function would be to begin the investigation, to include who is doing the attack and where it is originating from. A possible way to manage the attack would be to implement a man-in-the-middle attack against the attacker. Here the organization would no longer be at risk but the attacker would not know the difference while they are being investigated. Also, to add to their job role the tiger team would not have any jurisdictional or procedural boundaries to prevent a full investigation. (Colarik)

On a worldwide scale side each Internet Service Provider should require 100% authentication. No open authentication should be allowed. All users should be required to obtain digital certificates for who they really are and be required to have everything that leaves their computer be signed with their signature. In the event of an attack everything would be traceable, and assurance of who really did something would be proven by signatures. In addition to ensure the signatures are not forged, a special bit should be injected into the header of every packet that has the source computer's MAC address, and for it to be a different value if the packet is altered.

With the September 11th terrorists attacks we, as a nation, thought we were prepared for such an event with plans and policies, but in hindsight there was much confusion and panic. With proper training and preparation, confusion and panic would be removed from the scenario so the disastrous outcomes that were sure to occur will be minimal. With the above information the concept of cybercrime and cyberterrorism is a true and realistic fear that is eventually inevitable to happen. The difference we have as a nation is preparedness.

References:

Armistead, E. Information Warfare. Washington, D.C.: Potomac Books, Inc., 2007.

Colarik, Andrew. Cyber Terrorism: Political and Economical Implications. Hershey: IDEA Groupd Publishing, 2006.

Krasavin, Serge . "What is Cyber-terrorism?." Computer Crime Research Center. 8 Mar 2008 <http://www.crime-research.org/library/Cyber-terrorism.htm>.

Sectools.org Top 100 Network Security Tools. Insecure.org 8 mar 2008 <http://sectools.org>.

Waltz, Edward. Information Warfare Principles and Operations. Boston: Artech House, 1998.

Watson, Dale. "Congressional Testimony." Federal Bureau of Investigation. 06 Feb 2002. 8 Mar 2008. <http://www.fbi.gov/congress/congress02/watson020602.htm>

Weimann, Gabriel. "Cyberterrorism: How Real is the Threat?." United States Institute of Peace. 24 Dec 2004. United States Institution of peace. 8 Mar 2008. <http://www.usip.org/pubs/special/reports/sr119.html>.