Global Information Assurance Certification Paper

George Ballesteros **GSEC Practical Assignment 1.2b**

Cyber-terrorism and Information Security

Nightmare…

Take a second and just imagine… You wake up one day, grab your cup of coffee and head out to what you expect to be a typical day at work. After dealing with the hustle and bustle of everyday traffic, you get to your desk, turn on your PC and off you start checking & responding to e-mails, voicemails and the slew of other methods of communication. However as you go along, you notice things start to go wrong. Your e-mail system seems to stop working. Whenever you make a call you get a recording saying that circuits are busy. You try to use you cell phone and calls don't go through. You try to surf the Web and sites are taking forever to load. At this point, you start to panic because these "glitches" are causing the deal you've been working on the last few months to collapse and fall through and you feel hopeless. By the end of the dismal day, you eventually get home turn on your cable TV and the reception seems spotty. This is the last straw and you decide to head in early. It isn't until the next day you learn that hear the following:

> *"Without warning, several major U.S. cities suffer a series of mysterious, hacker-caused blackouts. Both Hizbollah and Hamas take credit, but the authorities aren't sure they actually caused the outages. Some say the attack is Iraqi-inspired; others say Iran is secretly behind the attacks to draw the U.S. – the "Great Satan" into still another military confrontation in the Middle East. While the besieged cities wrestle with these catastrophes, a terrorist in a van with laptop computer and antenna directs a Radio Frequency weapon at three sophisticated airliners sending all three plunging to the ground.* [1]

The government has stepped in to investigate what is called a "nationwide cyber-terrorist attack". The only thing you ask is "What is that and how did it happen?"

Does this scenario seem unrealistic? Some Americans and even a number of information technologists (IS) might think so. Just as only a few years ago most Americans didn't believe that we could have a terrorist attack on US soil, so do they believe that an attack such as the one above is unlikely. However, as many Americans learned from the World Trade Center and Oklahoma City bombings, there must be a general understanding that the feasibility of such an attack is real and we must learn to protect against it. In this paper, I'd like to discuss what cyber-terrorism is, its various forms, its effects, who is a terrorist, and how we, as information security specialists (ISS), could protect against it.

So what is cyber-terrorism?

The definition of terrorism as described by the FBI is "the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives."[2] Therefore cyber-terrorism (CT) can be defined as "the use of computing resources to intimidate or coerce others." [2]

When most Americans think of what a traditional terrorist attack is they may think of a bombing, an assassination, highjacking, or a kidnapping. However these are not the only forms of terrorism. They only happen to be the most common. What about CT? The most visible attacks we might consider are those to politically based websites and systems, but does it only consist of these types of attacks? Unfortunately the answer is no. Just as real world terrorism has many forms, so does CT. What other forms are there? CT attacks can be performed through, cyber-plague infections, web hacks, exploited system vulnerabilities, DOS attacks and any other number of similarly related activities. Anyone can be a target including governments, corporations, business, & individuals. As long as the activity coerces someone to act or believe something through fear and intimidation, then it might be considered CT. Does the activity have to have a politically or socially message behind it? Again, the answer is no. Just as real world South American guerrillas have made kidnapping a lucrative "business" to finance their activities, CT can be financially motivated. If we then take this a step further, in its broadest form, CT can include almost any form of cyber-crime.

(For general examples of cyber-terrorism, please visit http://www-cs.etsu-tn.edu/gotterbarn/stdntppr/cases.htm)

Why should I worry about CT?

With this definition in mind, we could conceivably consider that CT activities are literally taking place all over the globe on a daily basis. From the latest intrusion attacks into a company to the newest macro virus being released into the "wild", all these activities "coerce" business, governments, & individuals to change our daily normal activities, whether the acts are politically or socially/economically based or whether they are intentional or not. Just as the real world terrorist acts have forced our society to become more cautious at airports, public places and such, CT has forced business and individuals to change the way they work and communicate with each other.

The effects of CT are very much felt in today's society. Due to the fact that these attacks can be seen not only in foreign far-away countries but also in our own "backyards" (places where we do business, our jobs, our homes), there is a sense of insecurity and anxiety created. Rather than seeing computers and the Internet as the idealistic **safe** resource/ communication/ business tool it was created to be, it has grown to be an effective tool, which we need but against which we must also protect ourselves. Out of this insecurity, society has built up a mechanism to help deal and protect us from this reality. In the last ten years we

have seen countless books, articles, movies, headlines, investigative reports, and even whole sectors of the computing industry based on the anxiety & fear of the unwelcome and unknown. The effects are so deep that now words such as "computer virus" and "hacker" are now a common part of the English language.

Apart from the emotionally and psychological consequences on society, there is the economical effects. There have there have been reported instances where either individuals or institutions have paid millions of dollars to cyber-terrorist as ransom for threats made against them. Take for example the following statistics out of Great Britain.

> *"According to a source in Great Britain, terrorists have gained at least up to 400 million pounds from 1993 to 1995 by threatening institutions. Over the three years, there were 40 reported threats made to banks in the U.S. and Britain. In January of 1993, three separate incidents took place in London. During the sixth, a brokerage house paid out 10 million pounds after receiving a threat and one of their machines crashed. On the fourteenth incident, a blue-chip bank paid blackmailers 12.5 million pounds after receiving threats. Another brokerage house paid out 10 million pounds on the twenty-ninth incident…A Russian hacker, for example, tapped into Citibank's funds transfer system and took $10 million."* [2]

Just alone from the incidences mentioned in the above example, £42.5 million was paid out in only 4 out of the 40 reported cases. What about the other 36 cases? How about the **unreported** cases? How much was paid out for them? As you can deduce, the actual amount paid during that period for all CT attacks could very well double or even triple the figure mentioned and these statistics are only from two countries. Think of what the amount can be worldwide.

Now some people may think, "Ok. A lot of money was paid, but that still doesn't affect me. I'm just a regular Joe Smith." Again, the effects are deeper then what one thinks. Just as the cost of a petty crime such as shoplifting eventually is transferred to the customer, so is the cost of CT. The cost of replacing the lost funds, money spent in implementing a more secure environment, loss of revenue due to a smaller market share resulting from negative press, and other expenses are transferred over to the customer based in the form of higher fees for services and products. If the loss is significant enough, a company can fail and the effects are even greater due to the loss of jobs and similar consequences. If you're still not convinced, consider the effects of the opening scenario. What would happen if you lost e-mail for a day? How about not being able to make a phone call? Combine an Internet disabling attack with a strike against any of the nation's infrastructure systems (eg. telephone, energy, transportation, etc.) and the

results are devastating. When attacks reach this level of magnitude they can be classified as cyber-warfare.[3]

Who can be a cyber-terrorist?

Regrettably, the answer to the questions is anyone can be a cyber-terrorist. Though an attack as sophisticated as the one mentioned in the introduction is usually reserved for a well-organized and well-financed hostile group or nation, the proliferation of readily available hacker tools and "how-to" sites makes this not necessarily true. For example, in February 2000, several high profile websites (Yahoo!, Amazon.com, eBay, Excite) experienced what was a well-coordinated distributed denial of service attack (DDos). Eventually it was determined that the perpetrator was an overzealous 15-year old Canadian boy with a computer.[3] Below is a comment made to ZDNet's website regarding the potential effects of the 4-hour DDos induced slowdown/outage upon Yahoo! :

> *"You're talking about one of the biggest sites on the Web going down in the middle of the business day," said Malcolm Maclachlan, media and e-commerce analyst for International Data Corp. "That's pretty significant." Maclachlan says the approaching Valentine's Day holiday will likely make the e-commerce losses on Yahoo!'s shopping site even more dramatic. Maclachlan estimates Yahoo! typically does "millions of shopping dollars in a four-hour period."* [4]

The fact the attack was performed by an adolescent isn't surprising. According to the head of network security at M.I.T., Jeff Schiller, "most of the crackers we are dealing with are not experts, they are not very sophisticated…They do most of their cracking by downloading free hacking software from hacker Web sites." [5]

What can we do to protect ourselves?

Generally, there are a number of things we can do to protect ourselves. First and foremost, people must come to believe that cyber terrorism is real and not only reserved for government and Fortune 100 companies. Though they tend to be bigger targets for the malicious hacker, they are not the only targets. With this said, the next step is to go ahead and protect your site with the variety of tools available in the market place. If we take this a step further, one should learn to be proactive (rather then reactive) in protecting one's network. It makes life much simpler when trying to prevent an attack from occurring as opposed to discovering an attack, investigating the damage, and then preventing it from happening again. Of course, being proactive involves an essential step in Information security, training.

Lastly, once a security system and policy is in place, the next step is vigilance. Among the items that entail vigilance are the review of daily logs, performance of software updates, investigation of the latest hacker attacks and tools, & periodic revision of the security systems.

Having talked generally about protection, let us look at some particular actions. In his article "*Cyber terrorism, information warfare, and attacks being launched now and in the future in the heartland of America*" [1], Dave Pettinari complied the following list of to help guide us in protecting our networks:

1. *A security model that separates information in three categories: critical, sensitive, and public domain; with appropriate hardware/software security for each level.*
2. *Strong passwords.*
3. *Physical protection of good hardware and protected cabling.*
4. *Firewalls between the network and outside.*
5. *A good security policy with employees trained to appreciate its finer points.*
6. *Audit trails for logins, operation of files, and successful/unsuccessful accesses (lots of attacks come from within).*
7. *An intrusion detection system to identify harmful or malicious activity.*
8. *Encryption to prevention interception of vital information.*
9. *Workstations without disk drives and control/accountability of floppy disks to prevent evaporation of extremely sensitive information.*
10. *Dial-up and Internet-access restrictions (For example, three attempts to get into our system and you are locked out prevents war dialing programs from hammering their way in).*
11. *Background checks on personnel.*
12. *Technical training and security awareness for all staff.*

If we examine this list more carefully you will notice that it reflects many of the best practices that an information security specialist should follow.

"Ok, I'm doing everything on the list and then some. My computers are pretty secure. What else do I do?" As an individual it may be hard to do much more than what you have control over but as trained and responsible information security specialists, we have an obligation to helping others who are more vulnerable. How? By sharing information, participating in forums, newsgroups, and other security related events, and promoting the proper information security procedures, we secure, not only others, but eventually the nation's infrastructure. Unfortunately, it has taken some high profile & highly damaging intrusions to have business and government dedicate the necessary resources to bring us where we should be. For example, eWeek has reported the following:

"It took the globally debilitating "ILoveYou" virus and its link to vulnerabilities in the Outlook messaging software, but Microsoft Corp. says it has finally seen the error of its ways.

As a direct result of the infamous virus that struck one year ago… the Redmond, Wash., software giant has been quietly implementing a far-reaching strategy to build security into every piece of software it develops. To be sure, the shift is a dramatic one for Microsoft, which for years has focused its development efforts on ease of use… (The) company executives hope the moves… will help Microsoft to shed its reputation for being aloof about security… The security edict came straight from the top of the company following last year's Love Bug attacks…. The initiatives, which were revealed here at the show, mark a 180-degree turnaround."[6]

The next step…

As we have seen, cyber-terrorism is a complicated subject that is essential for information security specialists to understand. One must be aware of all of its aspects in order to better analyze how and where the "terrorists" are likely to attack our systems. What makes this subject critical is that a CT attack is relatively very easy and economical to launch. Therefore, it can from any where in the world, at anytime, and, more importantly, the stakes of this cat and mouse game are can be relatively very high. Since it is only a matter of time before a system gets attack we must remain vigilant and share the knowledge we obtain so that we can help protect ourselves at a personal, business, and national level.

References

1. Cmdr. Dave Pettinari. "Cyber terrorism, information warfare, and attacks being launched now and in the future in the heartland of America". Police Futurist International. Document Date Unknown. (URL:http://www.policefuturists.org/fall97/terror.html)

2. Author Unknown. "Cyber-terrorism" Document Date Unknown. URL:http://www-cs.etsu-tn.edu/gotterbarn/stdntppr/index.htm

3. Margaret Kane, "'Mafiaboy' busted in DoS attacks". ZDNet News. April 19, 2000. URL:http://www.zdnet.com/zdnn/stories/news/0,4586,2552467,00.html

4. Jennifer Mack, "FBI talks with Yahoo! about attack". ZDNet News. February 7, 2000. URL:http://www.zdnet.com/zdnn/stories/news/0,4586,2434394,00.html

5. Author Unknown. "Hacker Profile". Online News Hour. June 1998.
URL:http://www.pbs.org/newshour/bb/cyberspace/jan-june98/hacker_profile.html

6. Dennis Fisher & Scot Petersen, "Microsoft wakes up to security". EWeek. April 16, 2001.
URL:http://www.zdnet.com/eweek/stories/general/0,11011,2708065,00.html