Global Information Assurance Certification Paper

Countering Cyber Terrorism Effectively: Are We Ready To Rumble?

Shamsuddin Abdul Jalil

GIAC Security Essentials Certification (GSEC)

Practical Assignment

Version 1.4b

Option 1

June 2003

Executive Summary

Cyber terrorism is gaining tremendous attention nowadays due to the increasingly high amount of coverage being given to the subject by the media and various institutions especially those from the public and private sectors. They recognize the disastrous impacts that cyber terrorism is capable of realizing and thus it is very important to increase awareness on the subject among the general public in order to mitigate the threats posed by cyber terrorism more efficiently.

This paper discusses the various issues regarding the importance of protecting national and business interests from suffering the ill-effects of cyber terrorism. This paper is going to touch on issues such as identifying the main perpetrators of cyber terrorism and the motivations and common traits of such attacks. This paper will also discuss the different types of cyber terrorism attack and its effects on critical infrastructures and businesses as well as the psychological effects that these attacks have on humans. In addition, this paper will include the vital steps that can be taken to protect ourselves from cyber terrorism attacks.

It is expected that this paper will be able to provide its readers with a better understanding of what cyber terrorism is all about and assist them in identifying the steps that can be taken to address the threats posed by cyber terrorism effectively.

1. What is Cyber Terrorism?

A report published by PCWorld.com online magazine in 2001 stated that the Federal Bureau of Investigation (FBI) and the System Administration, Networking, and Security Institute (SANS) had released a list of the 20 top vulnerabilities of Internet-connected systems and urged organizations to close the dangerous holes in order to avoid major cyber terrorism attacks. According to Allan Paller who is the SANS Institute Director in the article, "The Internet is simply not ready because of these vulnerabilities; we're not ready to withstand a major attack". [1]

We cannot help but agree with Allan's opinion in the matter. Due to the vast and open nature of cyberspace, we would find it extremely difficult to defend ourselves from cyber terrorism attacks. Thus it is imperative for us to look deeper into the issues in cyber terrorism and understand them well in order for us to protect our nation's, businesses' as well as our personal interests from cyber attacks.

Cyber terrorism can be defined as electronic attacks from cyberspace from both the internal and external networks, particularly from the Internet that emanate from various terrorist sources with different set of motivations and are directed at a particular target [5]. The cyber terrorists generally perceive their targets to be either high-profile components of a nation's critical infrastructures or business operations. The main objective of these terrorists is to inflict damage which will either compromise or destruct targets in order to cause major physical and psychological impacts to them.

According to Clifford A. Wilke, "The ultimate threat to computer security is the insider" [2]. It is a well known fact that most cases of security breaches happen from inside the organizations. Thus cyber terrorism can also happen in the form of electronic attacks by authorized insiders, where the terrorists have obtained inside access to networks and systems via various means such as employment with the particular organization and others. This type of internal attacks is much more dangerous that the external ones because of the obvious difficulties in detecting them.

Besides direct internal attacks from insiders, insecure arrangements with outsourcing companies that employ or have been infiltrated by terrorists can prove to be dangerous as well [9]. Thus it is imperative that efforts to tackle cyber terrorism effectively should start from the roots, which means organizations need to place equal, if not more importance on securing themselves internally as well as externally.

2. Who are the cyber terrorists?

In order to defend ourselves from cyber terrorists, we will need to identify who they are in the first place. The threats of cyber terrorism can be inflicted by anyone with hostile intents that has access and knowledge of utilizing cyber capabilities such as amateur and professional hackers, disgruntled employees, cyber criminals, cyber terrorist groups and others.

The graphic below shows that amateur hackers are by far the biggest threat on the Internet at the current time. They are responsible for about 90% of all hacking activities [3].

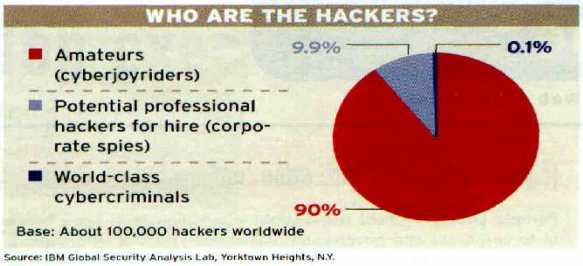

Figure 1: Distribution of Hackers in Cyber Terrorism

The fact of the matter is, the threats of cyber terrorism can come from so many different sources, and sometimes it would seem to be such an impossible task to actually defend ourselves from it. However, with proper planning and strategic security implementations, we would be able to significantly reduce the chances of cyber terrorism attacks from happening to us.

3. Motivations for Cyber Terrorism

There are many different motivations for terrorists to deploy cyber terrorism as a mean to inflict damage or destruction to their targets. The are four main goals for such attacks to be carried out by terrorists: to destroy enemy's operational capabilities, to destroy or misrepresent the reputation of an organization, nation or alliance; to persuade those attacked to change affiliation, and to demonstrate to their own followers that they are capable of inflicting significant harm on their targets [5].

i. To destroy enemy's operational capabilities

Cyber terrorism is deployed mainly for this particular reason. The terrorists feel that the usage of cyber capabilities offers them a low cost and effective solution to severely damage or destroy their targets in order to force them to be unable to continue their normal operations. The consequences of such attacks, if successful can prove to be very damaging in various ways including major collapses in economical and social standings. If critical infrastructures and business operations are hit, it can literally bring an entire nation or business to a halt.

ii. To destroy or misrepresent the reputation of an organization, nation or alliance

This is also one of the main goals of cyber terrorism. Many organizations, nations and alliances are able to operate effectively and are highly respected and regarded because of their unmistakable and strong reputation. If this vital element is tarnished, it could severely impact the normal operations of the targeted entity. The most common methods of destroying or misrepresenting the target's reputation include web site defacements and spreading false rumors concerning the particular target through electronic means such as e-mail, web sites and others.

iii. To persuade those attacked to change affiliation

Sometimes cyber terrorism is used in order to force the attacked entities to change their association or affiliation to certain parties. Even though this goal is much harder to be carried out, there has been cases where it has proved to be successful. Defending against such motivated attacks requires the attacked organization to form strong alliances with its partner entities in order to be able to handle the situation better or avoid such situations from happening altogether.

iv. To demonstrate to their own followers that they are capable of inflicting significant harm on their targets

Cyber terrorists are also keen to carry out cyber attacks because they want to prove to their followers and the world that they have the capabilities of inflicting severe damages on its targets. There are still a large number of people who are unconvinced about the realities of cyber terrorism and its capabilities. Thus if the cyber terrorists feel that they have a need to prove their capabilities of performing electronic-based attacks to their targets, they might do so to prove their "prowess" to the world.

4. Common Traits of Cyber Terrorism

Most cyber terrorism cases share several common traits. It is important to have a clear definition of what a cyber terrorism attack looks like in order to avoid misunderstandings which could lead to confusions later on. Usually, the victims of cyber terrorism attacks are specifically targeted by the attacker(s) for pre-determined reasons [8]. There has been random cases of attacks that have been carried out such as the release of harmful viruses and worms through the internet. However, in reality, the targets have been arranged earlier by the cyber terrorists. This is because most usually, if the attacks are more concentrated and aimed towards a specific target, there is a better chance of inflicting severe damages to that particular target.

The most common objective of cyber terrorism is to damage or destroy a specific target which may be an organization, industry, sector, economy or to just make an impact on particular targets [2]. This type of attack is becoming increasingly familiar nowadays and thus specific counter measures will need to be implemented to avoid the targeted entities from being victims of such an attack.

Another common characteristic of cyber terrorism is the purpose which is to further the terrorist or terrorist groups' own goals [8]; such as to inflict heavy damages to the previous employer due to unresolved disputes or to create chaos among the general public.

5. Types of Cyber Terrorism Attack

There are various types of cyber terrorism attack that are deployed by cyber terrorists. According to the Center for the Study of Terrorism and Irregular Warfare at the Naval Postgraduate School in Monterey, California, cyber terrorism capabilities can be group into three main categories; "simple-unstructured", "advance-structured" and "complex-coordinated" [4].

i. Simple-Unstructured

The capability to conduct basic hacks against individual systems using tools created by other people. This type of organization possesses little target analysis and command and control skills as well as limited learning capability.

ii. Advanced-Structured

The capability to conduct more sophisticated attacks against multiple systems or networks and possibly, to modify or create basic hacking tools. The organization possesses an elementary target analysis and command and control skills as well as relatively modest learning capability.

iii. Complex-Coordinated

The capability for coordinated attacks capable of causing mass-disruptions against integrated and heterogeneous defenses. The terrorists have the ability to create sophisticated hacking tools. They are also highly capable of conducting target analysis and command and control. They also possess advanced organization learning capability.

There are five main types of cyber terrorism attack which are incursion, destruction , disinformation, denial of service and defacement of web sites. Some of these attacks are more severe than the others and have different objectives. It is important for us to recognize the various methods of attack in order to gain a better understanding on how they can be countered effectively.

i. Incursion

These type of attacks are carried out with the purposed of gaining access or penetrating into computer systems and networks to get or modify information [11]. This method is very common and widely used with a high success rate. There are many loop holes existing in insecure computer systems and networks and terrorists can take advantage to obtain and/or modify vital information which can be used to inflict further damages to the organization or for personal gain.

ii. Destruction

This method of attack is used to intrude into computer systems and networks with the main purpose of inflicting severe damage or destroying them [2]. The consequences of such an attack can be disastrous, whereby organizations might be forced to be out of operations for an undetermined time, depending on the severity of the attacks. It can prove to be very costly for the affected organizations to get their operations up and running again and thus it will impact them hard financially and also damage their reputation.

iii. Disinformation

This method is used to spread rumors or information that can have severe impact to a particular target. Regardless of whether the rumors are true or not, the use of such attacks recklessly can create uncontrollable chaos to the nation or the organization. This type of attack is quite difficult to contain since it can be done almost instantly without the need to access the victims computer and network systems.

iv. Denial of Service

Denial of Service attacks or DOS attacks as they are more widely known are also a common method of attack. The impact of such attacks is felt the most by e-commerce enabled business that sells products or services online. Public websites are also sometimes the target of this type of attack by cyber terrorists. The main objective of DOS attacks is to disable or disrupt the online operations by flooding the targeted servers with huge number of packets (requests) which would ultimately lead to the servers being unable to handle normal service requests from legitimate users. The impact from such attacks can be disastrous from both an economic and social perspective where it can cause organizations to suffer from massive losses.

v. Defacement of web sites

This type of attack is targeted to deface the websites of the victims. The websites can either be changed totally to include messages from the cyber terrorists for propaganda or publicity purposes which might cause them to be taken down or to

re-direct the users to other websites which may contain similar messages. The number of cases of such attacks has dwindled in the past few years thanks to a greater awareness on the issue. However, a small number of such cases is still happening and thus proper security measures will need to be taken to try to avoid such embarrassing and financially disastrous situations from happening again.

6. Effects of Cyber Terrorism on Critical National Infrastructures

Even though there has not been too many obvious cases of cyber terrorism attacks affecting the critical national infrastructures, steps should be taken to prevent such occurrences from happening. The critical national infrastructures that might be affected by cyber terrorism includes electrical, telecommunication and water supplies, military operations, financial and banking institutions, schools and universities, hospitals and others. These infrastructures are generally well protected in most countries as the entire nation's operations depends on them. However, the level of security on these infrastructures can still be further improved in order to provide a tougher resistance block to cyber terrorists.

Cyber-terrorism can be in the form of one catastrophic attack on national infrastructure, or a series of coordinated, seemingly independent attacks [2]. I will provide three scenarios of how cyber terrorists might cause massive damages to the nation and its people if they are able to compromise the security of critical national infrastructures.

Scenario 1:

The operations of a utility company which specializes in electrical distribution that serves critical businesses is disrupted by cyber terrorists. The cyber terrorists manage to interrupt the distribution of electricity to the customers. This will of course cause a huge problem to the affected entities or areas to carry on normal operations and the normal way of life.

Scenario 2:

Cyber terrorists who are interested to gain some publicity released network worms and viruses targeted to disable the operations of a critical financial institution after identifying a major weakness in the firm's network architecture. The worms caused the computer systems to consume very large payloads making them unable to service requests from legitimate users. This will cause the entire network and computer systems to become practically useless. This will result in major losses financially and cause the firm's dependencies to under perform critical duties.

Scenario 3:

Cyber terrorists manage to disrupt the air traffic control systems causing the controllers to be unable to direct the airplanes in the required manner. This might cause the pilots to lose control of the computerized navigation systems on the airplanes and make their task of ensuring a safe takeoff and landing much harder.

Thus it is absolutely imperative that stringent measures are taken to protect the critical national infrastructures effectively in order to prevent such scenarios from being realized. This is because the impact of such destructive attacks can not only cause massive damage to the economy due to the unavailability of information dissemination and processing capabilities, but it will also cause loss of opportunities due to the inability to conduct business as usual and will further result in reputation loss as well.

7. Psychological Effects of Cyber Terrorism to Humans

Needless to say that if the nation's critical infrastructures or business operations get damaged or disrupted by cyber terrorists, the people who are directly affected will suffer tremendous stress psychologically. We cannot underestimate the impact that cyber terrorism attacks might have on people since different people react differently to such situations.

Some people who are directly affected by cyber terrorism in cases such as loss of vital company information that can be used to threaten the well being of the organization or the targeted person might result in the affected person(s) to be afraid and live under severe stress. The person(s) involved will suffer emotionally and this might affect the well being of his or her mental health.

In other cases where disinformation attacks using websites, e-mail and other electronic means might be carried out to dispel rumors about a particular situation, organization or person, it might lead to a chaos among the general public. People will panic and thus normal business operations and the normal way of life will be disrupted.

Thus it is imperative that the general public should be well informed about cyber terrorism and are able to identify the steps that can be taken in order to handle the concern better. The psychological issues regarding the effects of cyber terrorism on humans and ways to treat the related problems effectively should be discussed more often in order to provide a trustworthy and stronger avenue for people suffering from such concerns.

8. Strategies to Deal with Cyber Terrorism Threats

In order to counter the ill effects of cyber terrorism, strategic plans should be put in place to ensure the well being of the nation and its citizens. In the following

paragraphs, the steps that can be taken by the parties involved to deal with the threats of cyber terrorism effectively will be discussed.

i. Pursue and Prosecute the Perpetrators

The parties that have been directly affected from attacks by cyber terrorists should be more aggressive in pursuing the perpetrators [7]. Even though this exercise might prove to be costly, it will definitely be to the organization's advantage if they are able to identify the perpetrators and prosecute them to the full extent of the law. If there is an increasing number of such attackers that can be brought to justice, it might change the general mindset of the cyber terrorist community and they will need to think long and hard of the consequences of their actions if they are going to get caught. Thus it might prove to be a good way of decreasing the number of such attacks in the long run.

ii. Develop Best Security Practices

Organizations should ensure that they develop and deploy a tested set of best security practices suited specifically for their own operations. These activities will require a lot of coordinated efforts from all parties in the organization because security procedures should be followed by every department.

The developed list of the best security practices should cover all the aspects involved in information security. As a starting point, it would be a good idea to adopt existing international standard guidelines for information security such as ISO17799 or BS7799. These standards provide the detailed steps that should be taken to secure organizations from an information security standpoint. The organizations can later modify or improve on the provided guidelines and adapt it based on their own operations and needs in order to obtain the best results.

iii. Be Proactive

Organizations and the general public should be more proactive in dealing with cyber terrorism issues by keeping up to date on the latest information related to threats, vulnerabilities and incidents and they should be more committed in improving their information security posture. By being constantly aware of the various components of cyber terrorism that could directly affect us, we would be able to be implement stronger security measures that would reduce the chances of cyber attacks from happening to us.

Organizations should always be looking to improve upon their existing security infrastructure. Organizations should deploy multi-level security architecture instead of the single-tier ones in order to protect themselves better. Critical activities such as security audits should be performed more often to reduce redundancies in the security implementation [2]. It should be remembered that

security is a continuous process, not an off the shelf solution. Thus, in my opinion the best way to handle security is to be proactive about it .

iv. Deploy Vital Security Applications

The use of security applications such as firewalls, Intrusion Detection Systems (IDS), anti-virus software and others should be encouraged and in some cases, mandated to ensure better protection against cyber terrorism. Organizations should deploy both network and host-based IDS along with other security applications [2]. There should be personnel who are assigned to record, monitor and report all suspicious activities in the organization's network and with the aid of the latest security systems, all these tasks can be done much faster and simpler. The prevention and retention of critical information required for forensic analysis should be ensured in order to facilitate further investigations.

v. Establish Business Continuity and Disaster Recovery Plans

It is important that business continuity and disaster recovery plans should be in place in all organizations. These plans, to be included with incident response activities if not in existence, should be established and maintained. These plans should be rehearsed and tested at regular intervals to ensure their effectiveness.

The plans that are implemented should involve two main activities which are repair and restoration [5]. The repair activity should fix the problem in order for the function to operate normally. The restoration plans should be activated with pre-specified arrangements with hardware, software and service vendors, emergency services, public utilities and others.

vi. Cooperation with Various Firms and Working Groups

Organizations as well as the general public should establish working relationships or arrangements with public and private bodies that could assist with various issues related to cyber terrorism. These working groups can assist tremendously in activities such as developing standard guidelines on improving organizational security, developing disaster recovery plans, discuss on the emerging and rising issues in cyber terrorism and others. Thus by exchanging information on such issues on a regular basis, it would create a pool of much needed experts in the field of cyber terrorism in order to increase resistance in general from such attacks.

vii. Increase Security Awareness

It is important to increase the awareness on cyber terrorism issues to the masses. By educating them, they would realize the importance of defending themselves from such attacks and thus it would assist in developing communities that are more proactive in dealing with information security issues. Security

training programs can assist people to equip themselves with the right skills and knowledge that are needed to protect their computer and networks systems effectively.

viii. Stricter Cyber Laws

The government can assist in controlling cyber terrorism attacks by adopting and revising new cyber laws that will punish the perpetrators more heavily if they are involved in such activities. New acts to encourage the development of efficient cyber security practices and to support the development and permit the use of more effective tools for law enforcement should be introduced.

ix. Encourage Research And Development

Organizations especially from the public sector should support research and development activities of personalized security tools such as firewalls and IDS. The main advantage of pursuing this approach rather than buying off the shelf product is that it will leave the perpetrators in the dark over the actual capabilities that the targets possess, and this can be a huge advantage when dealing with such knowledgeable and experienced attackers.

9. Where is Cyber Terrorism Headed?

Due to the rapid advancements being made in the world of Information Technology in general and in Information Security specifically, we have to accept the fact that cyber terrorism is only going to get more popular in the future. Due to the relatively low costs and simplicity in initiating such attacks and with an ever increasing number of highly skilled professionals in the computer field, cyber attacks will be a normal occurrence in the future.

Having mentioned that, I also believe that with the implementation of strategic security measures, increase in the number of user education and awareness training programs, and more collaboration between the industry, government and the general public, we would be able to protect ourselves better. This is because the parties involved will be in a better position to defend against cyber attacks more effectively having learned the necessary skills and knowledge to secure their infrastructures and operations well. As more and more information regarding cyber terrorism become known to the public, the community will be better prepared for it by implementing stringent security measures, adopt a tested best security practices plan and reviewing them more often to ensure its effectiveness.

The battle against cyber terrorism is going to be continuous one and we must be prepared to focus more on the aspect of information security when performing the various activities in our daily lives. Hopefully, with the above-mentioned steps

being taken, we would be able to deal with the emerging cyber terrorism issues in a better way and come-out victorious in the end.

10. Conclusion

Even though the field of cyber terrorism is relatively new to most of us, it has proved to be a very challenging one. So far, significant progress has been made through industry and government initiatives in many countries to protect against cyber attacks.

It is widely accepted and well known by everyone that security is not a one-stop solution. Instead it is a continuous journey that requires everyone involved to be committed to it. The many aspects connected to cyber terrorism such as understanding the different motivations and types of attack, realizing its effects on critical infrastructures, businesses and humans, as well as undertaking the sometimes complex steps to decrease the chances of such attacks from happening makes the task of protecting against it such an enviable one.

However, the implementation of strategic security measures and improved working relationships among the various bodies including the industry, the government and the general public provide all of us a strong hope of winning this battle. The fact of the matter is, cyber terrorism is here to stay and we still have a long way to go in protecting the nation's, businesses' and our interests effectively against it. The good news though, with the various strategic plans in place, we are getting closer to achieving our main objective which is to have a highly secure and productive working environment.

References

1. Thibodeau, Patrick. “Internet Vulnerabilities to Cyberterrorism Exposed. “ 1 October 2001. URL: http://www.pcworld.com/news/article/0,aid,64224,00.asp (4 June 2003)

2. A. Wilke, Clifford. “Infrastructure Threats from Cyber-Terrorists.” 5 March 1999. URL: http://www.occ.treas.gov/ftp/bulletin/99-9.txt (8 June 2003)

3. Sproles, Jimmy; Byars, Will. “Statistics on Cyber-terrorism.“ 1998. URL: http://www-cs.etsu-tn.edu/gotterbarn/stdntppr/stats.htm (5 May 2003)

4. E. Denning, Dorothy. Testimony before the Special Oversight Panel on Committee on Armed Services US House of Representatives. “Cyber terrorism.” 23 May 2000. URL: http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html. (18 April 2003)

5. Axelrod, C. Warren. “Security Against Cyber Terrorism. ” 27 February 2002. URL: http://www.sia.com/iuc2002/pdf/axelrod.pdf (6 June 2003)

6. Warren M.J; Furnell S.M. “Cyber-Terrorism – The Political Evolution Of The Computer Hacker.” July 1999. URL: http://www.businessit.bf.rmit.edu.au/aice/events/AICEC99/papers1/WAR99024.pdf (6 June 2003)

7. Erbschloe, Michael; Vacca, John. Information Warfare: How to Survive Cyber Attacks. Reading: McGraw-Hill Osborne Media, 2001. (18 February 2003)

8. E. Denning, Dorothy. “Is Cyber Terror Next?” 1 November 2001. URL: http://www.ssrc.org/sept11/essays/denning.htm (6 June 2003)

9. Glaessner, Thomas; Kellermann Tom; McNevin, Valerie. “Electronic Security: Risk Mitigation In Financial Transactions”. June 2002. URL: http://www1.worldbank.org/finance/assets/images/E-security-Risk_Mitigation_In_Financial_Transactions-3.0.pdf (7 June 2003)

10. Roos, Robert. “Disarmament and Security Committee: International Policies on Information Warfare.” 10 April 1998. URL: http://www.stanford.edu/group/smun/oldversion/oldversion/simun98/briefings/info-war.html (5 March 2003)

11. Noordegraaf, Alex. “How Hackers Do It: Tricks, Tools and Techniques.” May 2002. URL: http://www.sun.com/blueprints/0502/816-4816-10.pdf (7 June 2003)

12. NetXPress. “What is Cyber Warfare?“ 2001. URL: http://www.netxpress.com.pk/archives/articles/cwfa1.shtml (10 April 2003).

13. Report to the President's Commission on Critical Infrastructure Protection. "Threat and Vulnerability Model for Information Security." 1997. URL: www.ciao.gov/resource/pccip/ThreatVulnerabilityModel.pdf (11 April 2003)

14. Bryen, Stephen. ITU Workshop on Creating Trust in Critical Networks Infrastructure." A Global Security Approach to Protecting the Global Critical Infrastructure." 2002. URL: http://www.itu.int/osg/spu/ni/security/workshop/presentations/cni.20.pdf (13 April 2003)

15. M. Pollit, Mark. "Cyberterrorism - Fact or Fancy?" 1999. URL: http://www.cs.georgetown.edu/~denning/infosec/pollitt.html. (22 April 2003).

16. Phoenix Business Journal. "Government has role in fighting cyber terrorism." 2002. URL: http://personalweb.about.com/gi/dynamic/offsite.htm?site=http://sanfrancisco.bizjournals.com/sanfrancisco/stories/2002/12/02/editorial3.html (25 April 2003).

17. Krasavin, Serge. "What is cyber-war? " 27 July 2000. URL: http://www.crime-research.org/eng/library/Cyber-terrorism.htm (1 May 2003).

18. Shahar, Yael. "Information Warfare: The Perfect Terrorist Weapon." 31 October 2001. URL: http://www.ict.org.il/articles/infowar.htm (10 May 2003).

.