PREVENTING CYBER CRIME

Keywords: Cyber crime, Cyber security

The Lack of Attention in the Prevention of Cyber Crime and How to improve it

Brett Pladna

ICTN6883

East Carolina University

Abstract

This paper discusses the issues of cyber crime and what is being done to prevent it. Cyber criminals take advantages of vulnerabilities by using viruses, bots, etc to cause damage and/or maybe steal information. There are ways that this can be minimized by being aware of what the problems are. There are many problems but common ones are discussed. Not can these problems be solved on an individual or organization level but also on a global level. This paper will look at what cyber crime is and three topics that discuss the problems with cyber crime and how to prevent it.

Introduction

In today's world we use computers for everything; searching the internet, online shopping, accessing bank accounts, Email, and online gaming as some examples. Communication is faster and more reliable than in the past which has allowed more to be accomplished in a given day. The problem is just like anything else; vulnerability. There are individuals that hack into computers as well as the networks of businesses and government agencies. The problem is that sensitive data can be stolen and/or destroyed. There needs to be more focus on the security of computers and the internet. This paper will focus on the lack of efforts to prevent cyber crime as well as problems associated with it, how cyber security can be improved, and what has been done in response to cyber crime.

What is Cyber Crime

"Cyber crime is regarded as computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks. Cyber crimes describe criminal activity in which the computer or network is a necessary part of the crime" (Govil, 2007). From the definition it is obvious that the computer is the major source of cyber crime. Cyber crime is a growing list of internet-facilitated offenses.

Today street crimes are becoming something of the past. It is not to say that they don't occur but computer crime is more convenient. Govel (2007) said it "has proven to be accurate, easy, and reliable; detection has posed constraints in preventing cyber crime." Some of the constraints/characteristics are shown in Figure 1.

Figure 1:

1	Low marginal cost of online activity due to global reach	6	concrete regulatory measure
2	Lower risk of getting caught	7	Lack of reporting and standards
3	Catching by law and enforcement agency is less effective and more expensive	8	Difficulty in identification
4	New opportunity to do legal acts using technical architecture	9	Limited media coverage
5	Official investigation and criminal prosecution is rare; not very effective sentences	10	cyber crimes are done collectively and not by individual persons

(Govil, 2007)

There are different areas of cyber crimes shown in Figure 2:

Figure 2.

Financial	Using fake websites to market products so as to get the credit numbers
Cyber	Spreading child pornography or sexually implicit material

pornography	
Marketing strategies	Selling narcotics or weapons online
Intellectual Property	Software piracy, copyright infringement, trademark violations, theft of computer code
Email spoofing	Hacking email/password; sending unwanted message to others ruining a person's image
E-Murder	Manipulating medical records
Political	Abuse of public funds by altering data; bribery by altering data
Theft of telecommunication services	Gaining access to dial in/out circuits and using the phone lines like a calling card
Information piracy and forgery	Perfect reproduction of original documents such as social security cards, birth certificates, etc…
Money laundering and evasion	Bypassing the banking system and taxation authorities by concealing the origin of ill-gotten money
Electronic terrorism	Electronic intruding into government websites to bring them down
Electronic funds	Financial institutions use electronic fund transfer systems and

transfer fraud	hackers intercept them and divert the funds
Hacking	Information theft from computers, removal storage, stealing and altering information, etc…
E-mail/logic bombs	Event/date programs that do something when a certain event occurs
Internet time thefts	Stealing user name and password from user to use their account time
Hate/commercial	Building a website to promote hate or racial hate.
Altering websites	deleting web pages, uploading new pages; controlling messages conveyed by the website
Computer viruses	using malicious code or software to cause destruction to information

These are a lot of different areas of computer crimes which means there are many opportunities for a hacker to be successful. How they perform these crimes is another important issue. Knowing what they use will give us a better way to help minimize these crimes. “Unauthorized Access is the main tool used by Criminals. Unauthorized access means any kind of access without the permission of rightful owner or in charge of the computer, computer system or computer network.” (Govil, 2007).

Just like there are different types of criminals there are different types of cyber criminals. Kids enjoy hacking into computers and websites. They also commit cyber crimes without knowing the implications. Organized “hacktivists” use social activism and religious activism to attack prominent websites for political reasons. Disgruntled employees will commit computer crimes instead of going on strike. It is easier for them since a lot of the damage can be done with automation process. Finally, professional hackers can be an employee(s) of a company stealing information from a rival company(s). These hackers also employ their own methods of criminal success. They might use one or more of these techniques depending on what they are trying to accomplish.

The following are techniques used by hackers:

Packet Sniffing

This is used by hackers and forensic experts. Data travels in the form of packets and vary in size depending on the network bandwidth and amount of data. The hacker intercepts the transmission between computer A and B. All the hacker needs is the IP address from one of the computers and any data can be stolen. The data is not stolen because sniffers don’t do that. Instead they copy the hex and translate it into original data. This is why it is hard for firewalls to detect this because they only provide application level security.

Password Cracking

A password is a type of authentication. During login, the password is stored in memory. If a hacker has access to the computer during this time, they can sift through the memory for the password. Another method to find a password is “brute force.” This is trying to find every letter/number combination. These take much longer to figure out.

TEMPEST Attacks

This is an acronym for Transient Electromagnetic Pulse Emanation Standard. Data that passes though circuitry and mechanical devices produce electro-magnetic emanation. This allows hackers to monitor and put data from network cables. The hacker has to be in range of the network cables so they may be in a parking lot or adjacent room in the building.

Buffer Overflow

This is the most common way of breaking into a computer. Buffers are created to hold a finite amount of data. When it overflows, it goes into adjacent buffers which can cause data to be overwritten. In buffer overflow attacks, the extra data can contain instructions that trigger specific actions. These actions can cause damage to files and/or change data.

Lack of Efforts to Prevent Cyber crime

As with any type of crime there are problems. We know that there is not a way to completely eradicate crime but there is no excuse why some crime goes over looked. The biggest example is the United States Government. There has been little accomplished in the prevention of cyber crime in the government. In an article released in 2005 Paul Kurtz, head of the Cyber Security Industry Alliance (Cyber Security Industry Alliance, 2005) said that "Multiple data security breaches in the past year have exposed the personal details of over 50 million Americans" (New Scientist, Reed Business Information UK, Ltd, 2005). In the future if the problem is not addressed appropriately, then sensitive data such as medical and financial records could be in jeopardy. In December of 2005, the CSIA[1] gave the US government grades mainly consisting of D's and one F. The report makes 13 new recommendations along with a law that would require

[1] For more information on the CSIA go to http://www.csialliance.org/

companies to notify customers of any security breaches. Figure 3 shows the grades the US Government received in 2005. Also the 13 recommendations can be seen in Figure 4.

Figure 3.

Agenda 2005	Action	Grade
Establish a new cyber security post in the Department of Homeland Security	Secretary Chertoff announced creation of an Assistant Secretary for Cyber Security and Telecommunications; however this post has yet to be filled	**C**
Ratify the Council of Europe's Convention on Cyber Crime	Senate Foreign Relations Committee referred Convention to Senate for Ratification but no vote has been taken to date	**B**
Promote information security corporate governance in the private sector	Little to no action	**D**
Lead by example in federal procurement practices	OMB may establish a separate line of business for cyber security to promote more efficient and consistent security standards across government; and an interim rule under the Federal Acquisition Regulation requires agencies to plan for security and seek advice from security professionals, however enforcement is unclear .	**C**
Closing the strategic gap between the government and private sector information security efforts	The Federal government is too focused on collecting information relevant only to the security of national security systems; it must include data for the private sector to effectively improve information security	**D**
Strengthen information sharing	Little action by the Federal government while legal and organizational issues continue to cause uncertainly in the private sector slowing information sharing mechanisms	**D**
Establish and test a survivable emergency coordination network	DHS established the Homeland Security Information Network-Critical Infrastructure (HSIN-CI), but the network is Internet-based and subject to outage.	**C**
Direct a federal agency to track costs associated with cyber attacks	Little action, though DHS is sponsoring limited economic analysis of the cost of cyber attacks and Justice has initiated a survey on the costs to business of attacks	**D**
Increase R&D funding for cyber security	Despite a presidential panel that declared a crisis in cyber security R&D, funding remains flat and clear priorities absent	**D**
Fund authorized responsibilities for NIST and OMB	Appropriated funding does not cover statutory responsibilities for cyber security by these agencies	**D**
Improve the quality of software cyber security	A study by DoD and DHS on the effectiveness of NIAP was not shared with the public, so no data is available to show how NIAP	**F**

by strengthening NIAP Certification	certification improves information assurance	
Secure Digital Control Systems	DoE and DHS are creating a roadmap to secure energy controls and are funding digital control systems testbeds	**C**

(Cyber Security Industry Alliance, 2005)

Figure 4.

Privacy & Security for Consumers
Pass a national data breach notification bill
Pass a national spyware protection bill

Security & Resiliency of Information Infrastructure
Ensure cyber security protection be applied to healthcare infrastructure
Promote information security governance in the private sector
Direct a federal agency to track costs associated with cyber attacks
Secure Digital Control Systems
Improve quality of software cyber security by strengthening NIAP certification

Federal Information Assurance Initiatives
Fill new cyber security post in Department of Homeland Security
Ratify the Council of Europe's Convention on Cyber crime
Increase R&D funding for cyber security
Complete HSPD-12 initiative for government-wide authentication
Ensure continuity of government operations with telework
Include information security planning in transition to IPv6

(Cyber Security Industry Alliance, 2005)

Not only did the CSIA have a problem with how the United States Government had been handling the fight on cyber crime but Alan Paller did an interview discussing his thoughts as well. After the fifth anniversary of September 11th, he discusses his non-acceptance of the Government's policies to fight cyber crime.

The interview with Alan Paller (2006) is as summarized:

InfoWorld: We've been hearing about the threat of terrorist cyber attacks for years. Is the threat for real?

Alan Paller: It is a real threat, but it's an interesting threat. What you have happening today is that terrorists are using cyber crime to get the money to buy the bombs to blow people up. But they're not using cyber attacks against physical things. There have been two cases that are very secret where SCADA[2] systems that run power plants were taken over, but the crime was about extortion

— you know, 'If you don't pay us we're going to do something bad.' In some cases the guys have proven that they can do damage by running a test denial of service attack, or a test outage.

IW: If you had to give the U.S. government a grade on cyber security, what would it be?

AP: It would have to be an F. I mean, if you can't secure the boxes that you have, that would have to be an F.

(P. 1)

Alan Paller was an original member of the National Infrastructure Advisory Council which means he received almost the same information as White House officials. He is also a critic on cyber security. In this interview he mentions SCADA which is the Supervisory Control and Data Acquisition which is responsible for maintaining the nation's infrastructure. From his interview he said the nation's security is ineffective.

Besides the government there are also problems on the internet in regards to the general public. In the community, cyber crime is said to be more widespread, skillful, and dangerous than ever. The Director of the Rapid Response Team at VeriSign-Owned iDefense, Ken Dunham and his team are malware hunters. They go online and "infiltrate black hat hacker forums, chat rooms

[2] SCADA is an acronym that stands for Supervisory Control and Data Acquisition. SCADA refers to a system that collects data from various sensors at a factory, plant or in other remote locations and then sends this data to a central computer which then manages and controls the data.
For more information go to http://www.tech-faq.com/scada.shtml

and newsgroups, posing as online criminals to gather intelligence on the dramatic rise in rootkits, Trojans and botnets" (Naraine, 2006). After two years of work Dunham and his team were convinced that well organized crime groups had taken control of "a global billion-dollar crime network powered by skilful hackers and money mules targeting known software security weaknesses" (Naraine, 2006). Dunham said "There's a well-developed criminal underground market that's connected to the mafia in Russia and Web gangs and loosely affiliated mob groups around the world. They're all involved in this explosion of phishing and online crime activity" (Naraine, 2006). As frightening and surreal as the cyber crime problem is, it is worse in other countries. In Russia these criminals literally post stolen credit card numbers, Social Security Numbers, PayPal and eBay credentials. In Eastern Europe, Asia and Latin America there are skilled hackers that are selling same day exploits on internet forums. They even test the code against antivirus software so it has a better chance of being 100% effective.

Viruses, worms, and Trojan horses are another serious threat. There is a variety of Cyber crime committed but these are the most prevalent and appear to be among the most troubling to computer users (Furnell, 2002). What's worse is that victims of these crimes usually go uncompensated due to the difficulty in finding those responsible. Due to the inadequacy of existing laws, law enforcement agencies throughout the United States have been slow to respond to computer crimes or provide the necessary intelligence for better understanding these offenses (Hughes & DeLone, 2007). Viruses appeared in the 1980s but were not significant until the 1990s. Earlier viruses had to be propagated by means of external media (i.e. floppy disks). Today with the advancement of the internet it is possible to disperse these viruses anywhere where there is an internet connection. Unfortunately there is no centralized database that collects information on the damage that viruses cause. Usually each vendor keeps a list on their web site and updates

it as viruses are found. This along with reports from major virus companies about the substantial increase in the number and complexity of malware attacks in 2005 is reason for concern (Hughes & DeLone, 2007). A September 2005 *Internet Security Threat Report* also shows a "shift during the first six months of the year toward more profit-oriented attacks and attacks that target individual computers rather than the servers and networks to which they are connected" (Symantec, 2005). The money lost by individuals might seem substantial but is pale compared to that of the pecuniary losses incurred by corporations, government, educational institutions, hospitals and financial institutions. To show how serious the monetary loses can be a survey was done about the effects of viruses.

A survey found the following results (Gordon, Loeb, Lucyshyn, & Richardson, 2005):

Findings from the 10th annual Computer Crime and Security Survey, conducted by the Computer Security Institute in cooperation with the San Francisco Federal Bureau of Investigation's Computer Intrusion Squad, suggest that the fiscal losses to these entities are staggering. Respondents reported $130,104,542 in losses from 13 different types of computer security incidents, with the greatest amounts attributed to viruses ($42,787,767), unauthorized access ($31,233,100), and theft of proprietary information ($30,933,000).

(P. 83)

As you can see here, even though viruses are one of the most common attacks they can cause a lot of damage financially. Again, it may not be as noticeable to the home user who gets a virus every once in awhile but a corporation that has thousands of computers will take more time to recover.

Bots are another problem. A bot is an adversary or criminal that controls a computer remotely. When bots are grouped into more than one they are referred to as botnets. Today it is millions of bots that are grouped together. In the spring of 2007 the first cyber war was started in Estonia. The country defended itself for a month from denial of service attacks that clogged the country's servers, routers, and switches. "Although the attack originated in Russia, millions of bots from around the world were combined into a botnet, forming a giant network used to mount the assault" (Emke, 2008). Anyone who is networked is vulnerable to these attacks. In June of 2007 "an attack originating from China shut down the unclassified network in the Pentagon for a week" (Emke, 2008). Targets such as the Pentagon are one of many. Other targets for cyber attacks include power grids, energy infrastructures, banking and financial services, defense services and the defense industry, emergency response networks, and telecommunications. Andy Purdy, the former acting director for cyber security with the Department of Homeland Security, recently stated, "Nine out of 10 businesses in the United States were affected by cyber crime last year" (Emke, 2008). Finally, what makes these problems worse is that software development is globalized. The United States has been saving billions of dollars by outsourcing software development. Outsourcing and moving software offshore increases the threat of cyber attacks in the United States. Due to different laws intellectual property varies from country to country. This is why it would be a good idea for the world to have universal laws when it comes to the internet. Different countries enforce and apply laws differently. It may be illegal to pirate movies, music, and software but some countries are not as strict as others.

These are just some of the big problems that cyber crime has to offer. If ignored, these problems will only get worse. How these problems can be lessened is discussed next. It is important to realize how much these problems affect everyone. It may not seem to be a major concern for an

individual home user but if you think it about it this way; what happens when you order a product off of the internet from a major company. You are expecting it to be delivered in the time specified. What happens if that companies systems are compromised? You might not get your product on time. This is why it is important for everyone to be aware of the problem and try to help solve it.

How Cyber Security Can Be Improved

There are a lot of problems caused by cyber crime and from the information it is clear there needs to be more done to protect everyone from the disasters of cybercriminals. There are things that can be done to help prevent cyber crime from getting worse. Cyber crime won't go away completely but it can be lessened significantly. Bot attacks have become more common and as discussed previously they are very dangerous. What needs to be done is to implement the "strongest appropriate security measures" (Gibson, 2006). One measure that should be taken is protection of e-mail. A secure e-mail gateway would be appropriate since bots, viruses, spam, and phishing attacks are common. Token-based identity management might also be appropriate. Basic "token-identification works as follows- the third party app can direct users to a site, with some extra information identifying which app is contacting the site. The site makes the users log in, and once that user is logged in, they can opt to approve access to their account from your app. Once the user has logged in and approved your app for access to their account, the site sends back a special code that you can use to obtain a token for access to that user's account. That token will contain the user's information, as well as a special token code that you can pass to the site with every method that supports authentication, instead of passing a username and password directly. In this way, parties can both communicate without ever sending a user's password over the wire." (Yahoo.com, 2008) Although strong defense is good it is not enough. Legislation and

law enforcement must be involved. Congress considered the Personal Data Privacy and Security Act of 2005[3] (Now 2008) which "contains many measures that will help, including increasing criminal penalties for computer fraud involving personal data, invoking RICO (Racketeer Influenced and Corrupt Organizations) Act provisions in cases of unauthorized access to personal information, and making it a crime to intentionally conceal a security breach involving personal data" (Gibson, 2006). Unfortunately, it has not passed. It was scheduled for debate on May 23rd, 2007 but nothing has come of it as of yet (110th Congress, 2007).

A final improvement is in the technology industry itself. By looking at how to prevent cyber attacks we can also see how it can help a company economically. From a software project manager perspective you want to ask yourself two questions: what is the likelihood of an attack, and what are its likely consequences? Security analysts understand cyber attacks and the potential risk and damage that can occur but research on the economic consequences of cyber attacks has been limited. Managers know the effect of a cyberattack from one computer to another but do not know the direct and indirect costs. Since project managers do not have this methodology it is hard to make an informed decision on how much to invest in cyber security. The assumption is that the likelihood of cyber attacks are high and they might increase over time. There is evidence that shows that even organizations that have taken the proper steps to keep secure have had significant attacks.

Pfleeger and Rue (2008) said, "To provide a more realistic picture of the nature and number of cyber incidents, researchers have conducted several surveys in the last few years to capture information about security attacks and protection. The following are among the most well

[3] For more information on the Personal Data Privacy and Security Act go to http://leahy.senate.gov/press/200506/062905a.html

known:

Since 2002, the annual Australian Computer Crime and Security has used information provided by Australia's federal, state, and territorial law enforcement agencies and the national computer emergency response team AusCERT (www.auscert.org.au). It solicits data from large organizations about computer network attacks and computer misuse trends in Australia.

The UK Department of Trade and Industry has administered several Information and Security Breaches Surveys, or ISBSs (www.infosec.co.uk/files/DTI_Survey_Report.pdf), since 1991.

They report on Internet use, dependence on information technology, and computer security incidents at UK businesses.

The annual CSI (formerly CSI/FBI) Computer Crime and Security Survey (http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2007.pdf) polls computer security practitioners in US corporations, government agencies, financial institutions, medical institutions, and universities that have joined the Computer Security Institute or attended a CSI seminar or workshop. The survey addresses computer usage, attacks, and actions taken in response to security incidents.

Particular sectors have their own global surveys, such as the Deloitte-Touche Global Security[4]. For example, the third GSS, administered in 2005, solicited input from chief security officers and security management teams of financial services industry organizations worldwide, asking for their perceptions of how one organization's information security compares to its counterparts' security.

[4] To see this survey go to Survey www.dtti.com/dtt/article/0,1002,cid%253D172320,00.html

(P.35-36)

These surveys are inconsistent. The ACC reported a decrease in attacks while the ISBS found the percentage of attacked UK businesses had increased by a third over two years, and 43 percent of the CSI member organizations surveyed experienced increases in the rate of attacks. During this same time period, Deloitte-Touche found that the rate of security breaches in the financial sector to be the same. These variations could result from different factors such as “different countries, sectors, degrees of sophistication about security matters, and biases in the pool of respondents” (Pfleeger & Rue, 2008). This is one problem of determining how much cyber security can cost an organization. Another problem is the lack of defining, tracking, and reporting security incidents and attacks. The surveys taken vary from organization and results are rarely if ever comparable. These surveys are also based on respondents’ opinions, interpretations, or perceptions and not on solid data. A third problem is the source of attacks. The ACC survey report said the rate of insider attacks has remained the same while Deloitte said that the rate of insider attacks in the financial sector is rising. The EY also reported the raise of insider threats. There are other surveys that said other sources of attacks are unknown. The surveys generally agreed about the most serious attacks which are viruses, Trojan horses, worms, malicious code, insider attacks and phishing. Another variation in the surveys is the cost these attacks produce. “For example the ICSA survey has reported a 25 percent increase in the cost of recovering lost or damaged data. On the other hand, the ACC, EY, and CSI/FBI surveys found a decrease in total damage from attacks, even though this cost is increasing for some kinds of attacks (such as unauthorized access and theft, noted by CSI/FBI). Twenty-five percent of organizations reported financial loss to CSI/FBI, and 56 percent reported operational loses” (Pfleeger & Rue, 2008).

This information is needed for software managers so they can use it for preventing, mitigating, and recovering from attacks.

Software project managers need more data to support their decision about investing in security. Such data that is needed would be understanding current security practices; evaluating existing regulations and standards; choosing effective measures of effectiveness for resources allocation; choosing organizational structures to facilitate efficient use of resources; and understanding frequency and types of attacks. In addition to this data governments, industry, and monitoring organizations need to implement the appropriate standards and guidelines. The quality of software is dependent on patches, disclosure time of vulnerabilities. It is also important that vendors release their patches early rather than later. The more time it takes for patches to be released is more time for hackers to expose vulnerabilities and pass it on to other hackers. There needs to be employees of these companies testing software on a constant basis to insure integrity. If this means hiring extra employees then it might be worth paying that out in salary rather than getting an attack and having to shell out millions to repair the damage. It is also recommended that disclosure of vulnerabilities not be released. Releasing this information is telling anyone on the internet how to attempt to get into the software even if the vulnerability has been fixed. It gives opportunity to find more vulnerability.

The biggest problem as discussed is that the surveys are inconsistent even with more data there has to be other measures taken. Managers might need another instrument that is more accurate. It might not even be an instrument that is needed. It could be as simple as evaluating all electronic equipment connected to the network and internet and then determine how much it is worth and then decide how much security is needed. Software project managers cannot rely on data for

their security needs. Sometimes it just takes experience; time being in the industry. Figure 3 and figure 4 show ways to prevent cyber crime.

Figure 3.

Preventive Measures to Oppose Cyber Crime

Reduce Opportunities	Reduce Opportunities to the Criminals Develop elaborate system design so that hacker does not hack the computer
Use Authentication Technology	Use password bio-metric devices, finger print or voice recognition technology and retinal imaging, greatly immense the difficulty of obtaining unauthorized access to information systems. Attention to be paid to bio-metric technology as this recognizes the particular user's authentication for using the particular computer.
Lay a trap	Bait a trap to catch the attacker in our computer.
Develop New Technology	Develop Technology of encryption and anonymity and also for protecting infrastructure as hackers or cyber terrorists can attack over any nation's infrastructure resulting in massive losses.
Understand Cyber Crime	For volume, impact and legal challenges. Understand the benefit of proper equipment training and tools to control cyber crime.
Think about Nature of Crime	Computer crime is diverse, a deep thought to be given, what cyber crime can take place in one's particular organization, so that different types of monitoring/security system can be designed and proper documentation can be written for security system
Adopt Computer Security	Avail new sophisticated products and advice for computer crime prevention which is available free or paid in the market
Use Blocking and Filtering Programs	For detecting virus, since virus can identify and block malicious computer code. Anti Spyware software helps stopping the criminals from taking hold of one's PC and helps to cleanup the PC if the same has been hit.
Monitoring Controls	Separate monitoring to be done for (a) Monetary files (b) Business information.
Design Different Tools	For different needs rather than using one particular tool.
Data Recovery	Develop tools for data recovery and analysis
Reporting	Always report the crime to cyber fraud complaint center in one's country as they maintain huge data and have better tools for controlling cyber crime.
Educate Children	Children should be taught about the child pornography crime used by criminals and how to avoid that.
Design Alert Systems	Design the alert system when there is actual intrusion.
Install Firewalls	(a) As they block particular network traffic according to security policy. (b) Patches are generally installed automatically and automatically fixes the software security flaws.
Install Original Software	As they contain many security measures. Pirated softwares do not contain many security abilities which exist in the original software.
Online Assistance	Develop regular online assistance to employees. Learn Internet to one's advantage only and understand all tips to stay online safe.
Avoid Infection	Avoid infection rather than cleaning it afterwards Keep browser upto date for security measures.
Avoid bogus Security Products	As many anti-spyware activists' runs a website that list bogus security products. Read the license agreement before installing any program.
Attachments	Avoid opening attachments or e-mails which were not expecting and have come from unknown source or person.
Cross Check	Cross check regularly the statements of financial accounts and internet banking.

(Govil, 2007)

Figure 4.

Constraints and Suggested Measures for Law Enforcement Agencies

Lack of Funds (whereas law breakers have enough funds for best hardware and software)	• National Repository to be established for investigation into cyber crime. • More funds for training computer forensic personnel. • Sufficient funds to be kept aside every year for upgrading security system in future.
Lack of Latest Technology and Good Equipments	• Developing investigations tools for cyber crime in advance e-mail tracking. Investigators to be provided with latest equipments • Easy access to technology required, to conduct computer investigation • Use of specialized software and training.
Lack of Training	Investigators to be continuously trained for (a) proficiency in investigating cyber crimes (b) projecting the future complexes of cyber crimes (c) locating computer based evidences (d) understanding cyber crime legal challenges
Documentation and Procedures are not adequately Defined	• Describing advance search and seizure procedure in documentation to handle high volume crimes. • Since cyber crimes are diverse in nature different kinds of documentations are required for security system. • Reporting standards to be developed for investigating the crime.
Lacking Forensic Support	• Computerized forensic support required for making strong forensic imaging and verification. In order to follow 'footprints' both on the computer and on the Internet • Creating forensic software and using high storage hard drives and good equipments to maintain high standards for recovery and preservation of evidence
No Specialized Unit	• Creating cyber crime unit in the country • Creating emergency cyber response team • Provision of online assistance to all investigators
No Defined Jurisdiction	The victim and criminals are may be at two different places, may be overseas, hence adequate jurisdiction to be defined
Accountability	• Fixing responsibility on the investigator who investigates the cyber crime • Investigation report to be completed whenever a victims reports cyber crime rather than referring him to another agencies.
Lack of Manpower	• Sufficient and full time investigators to be assigned. • Specialized Investigators are required who have undergone proper training in investigating complex cyber crimes.
Lack of Centralized Information and Sharing/coordination	• Sophisticated crime to be centralized in order to conduct forensic computer investigation and access to a computer lab environment. • Law enforcement agencies should share information in the state and country so as to reach on the key point at the earliest. • Strong working relationship to be maintained with private sector for investigating the crime of mutual interest.
Lacking Storage Data Facilities	• Law & Enforcement agencies to store past and present data for predicting future attacks. • Large devices are required to store data.

(Govil, 2007)

Responding to Cyber crime

In response to cyber crime there have been laws that have been talked about in congress and around the world. One concern is that some of the laws around the world concerning the internet are different depending on the country. This not only gets confusing but it creates loop holes for criminals. What might be illegal in one country may not be a law or is not as heavily as enforced in another.

Satola (2007) says, "At the national level, various countries face different issues, depending, for example, on their level of development. This affects their enabling environment for access to and use of ICT4D[5], including the Internet. At the national level it is important to build capacity to address issues of a national dimension. At the international level, given that the Internet is a global phenomenon, countries must ensure that national policies guarantee interoperability, continuity, security and stability of the Internet and its applications. In certain areas (intellectual property and trade, for example) there are already consultative mechanisms at the international level. In other areas, as was pointed out in the WGIG[6] Report, there may be scope for improvement in or the creation of further consultative mechanisms to ensure interoperability, continuity, security and stability."

(P.52)

In response to a more unified regulation of the Internet, the WGIG was established by the Secretary-General of the United Nations on December of 2003 by the power given to him by the

[5] For more information on ICT4D see http://www.globalknowledge.org/ict4d/

[6] Working Group on Internet Goverance
For more information on the WGIG go to http://www.wgig.org
or for the actual report go to http://www.wgig.org/docs/WGIGREPORT.pdf

first phase[7] of the WSIS[8] that took place in Geneva. The WGIG met in June 2005 to discuss resolutions to a unified solution to governing the Internet. The WGIG discussed three topics: working definition governance; identifying public policy issues that are relevant to Internet governance and assessing the adequacy of existing governance arrangements; and Developing a common understanding of the respective roles and responsibilities of all stakeholders from both developed and developing countries. At the end of the meeting recommendations were given. These resolutions are still being discussed as of present time.

Around the world authorities have been responding to instances of cyber crime. There are a few notable incidents that show that there is progress being made and that there is zero tolerance for the crimes committed. The first case is about the FBI cracking down on cyber crime. 16 people were arrested from Poland and the United States for theft of personal data and phishing attacks. "Individuals were arrested in Atlanta and Columbus, Ohio. Raids were conducted in New York, Texas, Tennessee, Nebraska, Georgia and Ohio, the FBI said. Search warrants on three individuals in Romania also were performed this week as part of the ongoing investigation." (Swartz, 2006). This was one of the largest high profile cases. More than 100,000 credit card and debit cards from over 1,000 people were stolen and compromised. In 2004, the FBI and secret service disrupted forums dealing with stolen credit cards. *Shadowcrew* is one forum that had over 4,000 members. "Since then, other forums have formed or resurfaced with new security measures to avoid detection, security experts and law enforcement officials say." (Swartz, 2006).

[7] For Information on the first phase of the WSIS report go to http://www.itu.int/wsis/geneva/index.html

[8] World Summit Information Society
For more information go to http://www.itu.int/wsis/index.html

A second incident is cyber crime that took place in Seattle, Washington talks about how the FBI busted cybercrooks who were controlling networks with botnets. “"We applaud the government's involvement in stopping cyber crime," says Tom Gillis, senior marketing vice president at messaging security firm IronPort Systems.”But these arrests are a tiny drop in the bucket" (Acohido, 2007). Botnets are increasing but the more they happen, the easier it is getting for investigators to figure out what they will do and make it to stop them early. Anyone with suspected compromised computers is asked to contact their Internet Service Provider (ISP) and then file a complaint online to the FBI.

A final example of preventing cyber crime took place in Bogota, Colombia in March 2008. A gang called the Black eagles was being followed by authorities. Unfortunately they were very careful not to use cell phones and only used internet cafes to communicate. Years ago, Columbia authorities would have had no clue how to respond but with today’s technology they were able to call in the computer forensics team. They followed the gang members from café to café. A senior supervisor said, “We were able to reconstitute all of his activities, get enough information to locate people who cooperated with him, and make arrests,” (Whitelaw, 2008). Computer forensics is growing rapidly in Columbia because of the help of the Anti-terrorism Assistance program.[9] U.S. State Department’s Diplomatic Security Bureau. They have used these new skills against dangerous paramilitaries known as the United Self-Defense Forces of Columbia (AUC).[10] This group is one of the biggest drug trafficking organizations in the country of

[9] For more information on the ATA go to http://www.state.gov/m/ds/terrorism/c8583.htm

[10] For more information on the AUC go to http://www.nps.edu/Library/Research/SubjectGuides/SpecialTopics/TerroristProfile/Current/UnitedSelfDefenseForcesofColombia.html

Columbia. The government has been exposing many scandals involving politicians associated with this group due to the help of the U.S. trained computer forensic experts.

Whitelaw (2008) talks about one of the cases pertaining to one of the military leaders

Encryption

One of the early cases involved a paramilitary leader known as Jorge 40. In the spring of 2006, even as Jorge 40 and 2,500 of his followers were promising to demobilize, authorities were examining some of their laptop computers. "We did not have the tools yet," says Monica Camargo, the coordinator of cyber crimes at the Fiscalia, Colombia's corps of prosecutors, "but we did have some training." After borrowing equipment from the U.S. Embassy, her newly trained experts tried to break the encryption and reconstruct files that had been deleted.

Their findings were stunning--cocaine smuggling routes, names of allied Colombian politicians, even a list of 558 people slated to be killed. "They did talk about massacres," she says. "There were lists of jobs to be done." Today, a dozen Colombian congressmen are in prison, a former senator remains a fugitive, and hearings continue. "With the new training, they could get beyond the encryption that had been a stone wall," says Victor DeWindt, ATA program manager in Colombia.

Camargo's office was created to provide tech support but was transformed five years ago into a cyber crimes unit. At first, the unit downloaded free forensic software. The ATA program came along in 2005, offering training and specialized forensic equipment. The most important innovation was a special protective device to read, but not modify, hard drives, which insulates investigators from allegations of evidence tampering.

Even with U.S. assistance, Colombia's courts remain overwhelmed by the high crime rate and politically sensitive prosecutions, including the thorny parapolitics cases. Colombian officials say the prosecutions of prominent politicians are proof of their determination to root out corruption. But the scandal has also raised suspicions about just how high that corruption reaches--and whether the government and the courts can truly dismantle the paramilitaries. Adam Isacson, a Colombia expert at the Center for International Policy says, "Justice continues to be Colombia's Achilles' heel."

(P. 1-2)

As we can see, even though cyber crime is still a problem there have been some things that have been done to show criminals that the world has no tolerance for these crimes. There is still a lot of work to be done but it will take a lot of efforts; meaning if everyone can get with the same concepts of how to protect the internet then we are on the right path to minimizing cyber crime.

Conclusion

The problems with cyber crime; how to improve efforts of prevention; and the response to cyber crime are what help us to look at the dangers of cyber space. The Internet is a very powerful tool and effective means of communication but it is vulnerable just like anything else. The way to protect it for now is for everyone to be smart and follow preventive measures; individuals, institutions, and government alike should all follow these measures. We have seen the actions of the government and what bots and viruses are capable of and it is important that security measures be implemented. In response to these issues there have been requests from the WGIG as well as congres to implement more standards and laws to help minimize cyber crime. In response to some problems there have been efforts by some nations by arresting individuals and

groups that commit cyber crimes like the ones discussed earlier. If everyone does their part, not only will they be safer but it will be setting an example for others as well as making it more difficult for hackers to cause damage.

110th Congress. (2007). *S. 495: Personal Data Privacy and Security Act of 2007.* A bill to be made into a law, United States Congress, Washington, DC.

Acohido, B. (2007, June 14). Cyber crime arrests by FBI 'A tiny drop in the bucket'. (Final Edition).

Cyber Security Industry Alliance. (2005). *National Agenda for Information Security 2006.* Virginia: Cyber Security Alliance.

Emke, J. (2008). Trends and Shocks, and the Impact of the Acquisition Community. *Defense AT&L , 37* (1), 3.

Furnell, S. (2002). *Cyber crime: Vandalizing the Information Society.* Boston, MA, USA: Addison Wesley.

Gibson, S. (2006). *Stepping up the Effort to Beat Cyber-Crime.* Eweek.com.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2005). *CSI/FBI Computer Crime and Security Survey.* Sanfrancisco.

Govil, J. (2007). Ramifications of Cyber Crime and Suggestive Preventive Measures. *IEEE , 43* (4), 610-615.

Hughes, L. A., & DeLone, G. J. (2007). Viruses, Worms, and Trojan Horses: Serious Crimes, Nuisance, or Both? *Social Science Computer Review , 25* (1), 78-98.

Naraine, R. (2006, April 13). Cyber crime More Widespread, Skillful, Dangerous Than Ever. Retrieved April 1, 2008, from Eweek.Com: http://www.foxnews.com/story/0,2933,191375,00.html

New Scientist, Reed Business Information UK, Ltd. (2005). Gaping Holes in Internet Security. *New Scientist , 188* (2531/2532), 1.

Paller, A. (2006, September 11). Government Cyber security Gets an F. 1. (InfoWorld, Interviewer)

Pfleeger, S. L., & Rue, R. (2008). Cyber security Economic Issues: Clearing the Path to Good Practice. *IEEE Software , 25* (1), 8.

Satola, D. (2007). Legal Aspects of Internet Governance Reform. *Information Polity: The International Journal of Government & Democracy in the Information Age , 12* (1), 13.

Swartz, J. (2006, November 3). FBI Cyber Crackdown Leads to 16 Arrests.

Symantec. (2005). *Symantec Internet security threat report: Trends for January 05-June 05.* Cupertino, CA.

Whitelaw, K. (2008, March 10). Calling in the Cybercops. *144*(7). U.S. News & World Report.

Yahoo.com. (2008). *Upcoming API Documentation - Token-based Authentication.* Retrieved April 3, 2008, from Upcoming: http://upcoming.yahoo.com/services/api/token_auth.php