Global Information Assurance Certification Paper

SANS Security Essentials
GSEC Practical Assignment
Version 1.2d

A Call to Digital Arms

By

David A. Woody
May 16, 2001

The Internet is an unstable and insecure technology open to abuse and exploitation. As the systems used in both public and private organizations and in the management of infrastructures increasingly migrate to Web-based protocols, the potential for disruption increases. This disruption can be relatively low-level and non-threatening on a national security scale, for example in the case of the defacement of a personal Web site or a virus that clogs up e-mail inboxes. The disruption can also scale up to the level of interference with military communications, significant power outages, or important economic losses due to large-scale denial-of-service attacks, all of which have serious implications for national security. Imagine for instance a cyber-attack on the already fragile and overloaded power grid infrastructure system in California during peak demand for electrical power in July or August? The economic loss due to blackouts and the subsequent potential for public rioting is enormous and very real.

The rapid and omnipresent spread of modern information technologies has brought about incalculable changes in the nature of social interactions, economic transactions and military operations in both peacetime and war. The pervasiveness of the Internet has created significant personal, organizational, and infrastructure dependencies that are not confined by national borders. It has become a system of networks that is void of clear parameters or international legal consensus. Former President Clinton's $2 billion plan to combat cyber-terrorism and fight cyber-wars of the present and future is a glaring indication of the new global threats now facing the United States. This is a global issue and not limited to the United States alone, which makes this issue far more convoluted in that respect. Disruptive and destructive technologies are surging ahead so fast that our government is frequently focusing on already obsolete technologies and thus gets overtaken by events. Also more often than not our legal system is simply too bureaucratic and cumbersome, and the people within the legal system too technologically ignorant to keep up with the rapid onslaught of change in technology and its effect on society. Legislation is frequently being signed into law that is already obsolete in its ability to have any real effect. Largely the lawmakers themselves, who usually have little or no technical knowledge, are passing bills and legislation without fully understanding what impact the new laws will eventually have on our society. A clear example of that is HIPAA. The Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, which amends the Internal Revenue Service Code of 1986.

Title II of HIPAA includes a section entitled Administrative Simplification and requires the following:

1. "Improved efficiency in healthcare delivery by standardizing electronic data interchange.
2. Protection of confidentiality and security of health data through setting and enforcing standards.

More specifically, HIPAA calls for:

1. Standardization of electronic patient health, administrative and financial data.
2. Unique health identifiers for individuals, employers, health plans and health care providers.
3. Security standards protecting the confidentiality and integrity of "individually identifiable health information," **past, present or future.**"

HIPAA will cause sweeping changes in how all health care entities and administrative information systems will complete business and patient health information transactions. This will not be your one time event Y2K glitch and it's over. This law will impact our society forever. HIPAA includes all health care service providers and insurers, no matter what their size or function. HIPAA also calls for severe civil and criminal penalties for noncompliance. The fines can be up to $25K for multiple violations of the same standard in a calendar year, and up to $250K and or imprisonment up to 10 years for knowing misuse of individually identifiable health information. Compliance is mandatory and must be accomplished by January 2003.
http://www.hipaadvisory.com/regs/HIPAAprimer1.htm

Our Nation's Lawmakers original intent was to protect the rights of the individual when they wrote the security standards mandated by HIPAA legislation. Their mistake is that they did so without taking into account the enormity of the technical difficulties involved in a project of this magnitude. Especially when you consider the current state of insecurity on the Internet, as it exists within that technology nationwide. They made that mistake primarily because they simply did not truly understand the technology involved or what it will really take to bring all health care entities within compliance on time. Neither did they recognize the plethora of vulnerabilities within the very technology that they are mandating the use of to enact HIPAA, or that the evolution of that technology is exponentially accelerating so fast that our legal system simply cannot keep up with the changes. The end result when establishing laws in this manner is not always necessarily good for our society at large, no matter how noble the original intent. Personally, I predict that there will be lawsuits and litigation on an unprecedented scale. I believe that HIPAA legislation will make the tobacco industry's litigation problems pale in comparison. If you think our health care system is expensive now, just wait until the cost of HIPAA litigation starts to factor into the overall costs of future health care.

On another note almost all of the Fortune 500 corporations have been victims of cyber-crime whether they admit to it or not. The apparent ease with which cyber-criminals breached the security firewalls of Microsoft on October 25, 2000 and suspected of obtaining early sight of unannounced coming products, sent resounding alarms throughout the industrialized world's computer dependent economies. Obviously any unauthorized alterations to Microsoft's products would raise broad questions about the trustworthiness of some of the world's most widely used software applications. http://www.zdnet.com/zdnn/stories/news/0,4586,2645850,00.html

The majority of electronic "break-ins" are still not identified because:

1. Many management entities still refuse to devote adequate resources to basic risk-management.
2. Crackers (criminal hackers) have become increasingly sophisticated in their attack modes.
3. Law enforcement entities are not devoting sufficient resources to training electronic sleuths primarily due to under funding.
4. Adequate tools and or adequately trained Information Security personnel often are not available to accurately gauge the degree of intrusion.

Securing systems against intrusion is like trying to secure a military bunker that has over 65,000 doors and windows, each needing to be locked and then monitored 24 hours a day, every day. With that in mind there are five security goals that all networked systems should address which are availability, authentication and identification, confidentiality, integrity, and non-repudiation and each are defined as follows:

- **Availability.** The reliable access to data and services for authorized users. This includes the restoration of services after an interruption.
- **Identification and Authentication.** The process an information system uses to recognize an entity. Authentication establishes the validity of a transmission, message, or originator, and verifies authorization for the user to receive specific categories of information.
- **Confidentiality.** The assurance that information is not disclosed to unauthorized persons, processes, or devices.
- **Integrity**. The protection against unauthorized modification or destruction of information.
- **Non-repudiation**. Provides the electronic sender with proof of delivery and the electronic recipient with proof of the electronic sender's identity, so neither can later deny having processed the data.

Due to the complexity of the technology and inherent vulnerabilities that have evolved as Internet technologies rapidly move forward, it is becoming exponentially more difficult to establish and maintain those five security goals. The government has a paramount role in protecting and defending the Nation's civilian and military infrastructure and is sharing that burden through organizations such as the National Infrastructure Protection Center (NIPC). The NIPC serves as a national critical infrastructure threat assessment, warning,

vulnerability, and law enforcement investigation and response entity. The mission of the NIPC is to:

- "Detect, deter, assess, warn, respond, and investigate unlawful acts involving computer and information technologies and unlawful acts, both physical and cyber, that threaten or target our critical infrastructures.
- Manage computer intrusion investigations.
- Support law enforcement, counter-terrorism, and foreign counterintelligence missions related to cyber crimes and intrusion.
- Support national security authorities when unlawful acts go beyond crime and are foreign-sponsored attacks on United States interests.
- And coordinate training for cyber investigators and infrastructure protectors in government and the private sector."

http://www.nipc.gov/

Internet security is an integral part of our national security. Cyber security is now synonymous with economic growth and global free trade. To truly be effective, Internet Security requires unprecedented levels of funding and cooperation between the public, academic and private sectors. All three need to pool their collective practical, technical, theoretical and economic resources to combat this ever-growing problem. This is an extremely serious problem that has the potential to devastate our national security through cyber-attacks against our Nation's national infrastructure. More and more the private sector has become acutely aware of this and has chosen to be proactive in the matter. It is mostly Corporate America stepping up to the plate financially on this collective problem. Primarily because it has already cost them a fortune by doing business without taking into account their need for properly trained network security personnel to help mitigate the problem. Every enterprise system has some information that is confidential, and corporations should realize that Information Systems Security must be managed as an integral part of their business strategies to mitigate financial losses achieve maximum profit margin. Anything less will result in systems being compromised and the companies losing enormous amounts of money.

But the problem is much bigger than just at the corporate level. The growth of the Internet coupled with system users untrained in even the basics of how to properly update their anti-virus software much less other forms of layered defense strategies such as using a firewall system or disabling file sharing or even how to use Microsoft's Windows and Internet Explorer Update functions adds exponentially to the overall security problem. On top of that, more and more of these untrained Internet users are accessing the Web with high-speed broadband technology and are unknowingly providing more and more high bandwidth gateways from which to attack our Nation's critical infrastructure for the modern day cyber-enemy.

AT&T's own research describes the phenomenal growth in the Internet as shown here:

"Internet growth:
Is there a ``Moore's Law'' for data traffic?
K. G. Coffman and A. M. Odlyzko
AT&T Labs – Research
http://www.research.att.com/~amo/doc/internet.moore.pdf

> Internet traffic is approximately doubling each year. This growth rate applies not only to the entire Internet, but also to a large range of individual institutions. For a few places we have records going back several years that exhibit this regular rate of growth. Even when there are no obvious bottlenecks, traffic tends not to grow much faster. This reflects complicated interactions of technology, economics, and sociology similar to those that have produced "Moore's Law" in semiconductors.
>
> A doubling of traffic each year represents extremely fast growth, much faster than the increases in other communication services. If it continues, data traffic will surpass voice traffic around the year 2002. However, this rate of growth is slower than the frequently heard claims of a doubling of traffic every three or four months. Such spectacular growth rates apparently did prevail over a two-year period 1995-6. Ever since, though, growth appears to have reverted to the Internet's historical pattern of a single doubling each year.
>
> Progress in transmission technology appears sufficient to double network capacity each year for about the next decade. However, traffic growth faster than a tripling each year could probably not be sustained for more than a few years. Since computing and storage capacities will also be growing, as predicted by the versions of "Moore's Law" appropriate for those technologies, we can expect demand for data transmission to continue increasing. A doubling in Internet traffic each year appears a likely outcome."

Keeping in mind that currently the general consensus is that somewhere around 2.5 million host computers is being added to the Internet world-wide on a monthly basis and growing, versus only a few thousand people that are being adequately trained as Information Assurance Specialists for the entire year. And as if that isn't bad enough, throw in the fact that we now have bots to contend with.

With today's technology and easy access to automated programs we now have what are called bots, or short for robot. A bot is small script / computer program that runs automatically. Some bots are designed to automatically and systematically seek out computer systems already compromised or with system vulnerabilities waiting to be exploited, over the Internet. It will then automatically install another set of programs and software called a root kit. A root kit will then automatically inform its source programmer that a system has been compromised and waiting for further instructions. Full access and control of that system has been nefariously gained with the most minimal of effort. Therefore it is easy to deduce that if anyone connects an unprotected computer to the Internet it will quickly become compromised, probably within only a few minutes of connectivity if even that long. Remember the growth of the Internet? How many of those millions of new hosts added monthly do you think are adequately protected?

According to a government white paper written in December of 2000 and called "Global Trends 2015: A Dialogue About the Future With Non-government Experts", the National Foreign Intelligence Board under the authority of the Director of Central Intelligence and prepared under the direction of the National Intelligence Council, predict the following about Information Technology:

> "Over the next 15 years, a wide range of developments will lead to many new IT-enabled devices and services. Rapid diffusion is likely because equipment costs will decrease at the same time that demand is increasing. Local-to-global Internet access holds the prospect of universal wireless connectivity via hand-held devices and large numbers of low-cost, low-altitude satellites. Satellite systems and services will develop in ways that increase performance and reduce costs.
>
> By 2015, information technology will make major inroads in rural as well as urban areas around the globe. Moreover, information technology need not be widespread to produce important effects. The first information technology "pioneers" in each society will be the local economic and political elites, multiplying the initial impact.
>
> - Some countries and populations, however, will fail to benefit much from the information revolution.
> - Among developing countries, India will remain in the forefront in developing information technology, led by the growing class of high-tech workers and entrepreneurs.
> - China will lead the developing world in utilizing information technology, with urban areas leading

the countryside. Beijing's capacity to control or shape the content of information, however, is likely to be sharply reduced.
- Although most Russian urban-dwellers will adopt information technologies well before 2015, the adoption of such technologies will be slow in the broader population.
- Latin America's Internet market will grow exponentially. Argentina, Mexico, and Brazil will accrue the greatest benefits because of larger telecommunications companies, bigger markets, and more international investment.
- In Sub-Saharan Africa, South Africa is best positioned to make relatively rapid progress in IT.

Societies with advanced communications generally will worry about threats to individual privacy. Others will worry about the spread of "cultural contamination." Governments everywhere will be simultaneously asked to foster the diffusion of IT while controlling its "harmful effects.""

http://www.cia.gov/cia/publications/globaltrends2015/index.html

The Internet by its very nature is and likely will remain an unstable, immature, and insecure technology open to abuse and exploitation. Because hacker tools are increasingly cheap or even free of charge, accessible over the Internet, and easy to utilize as a "digital weapon" ideological radicals, terrorist organizations, and individuals can readily perpetrate disruptive cyber-attacks at will.

Numerous types of threats are emerging from this new environment, each with varying levels of national security concern:

- The threat of disruption of communication flows, economic transactions, public information campaigns, electric power grids, public transportation and political negotiations.

- The disruption of military communications in times of conflict presents the potential for loss of life or aborted offensive missions. The probability of this type of threat materializing is considerable, as the tools required to create disruptive viruses and denial-of-service attacks are rudimentary and pervasive. Many well-documented events such as these have already taken place with economic consequences in the United States measured in billions of dollars.

- The threat of exploitation of sensitive, proprietary, or classified information and information theft, fraud, and cyber-crime can have extremely serious effects at personal levels such as identity theft, at institutional levels such as online credit

card fraud or theft of thousands of credit card numbers, and at national security levels when classified or unclassified but sensitive government systems are systematically probed. This threat is made all the more ominous by the difficulty in detecting these types of intrusions and compromised systems.

- The threat of manipulation of information for political, economic, military, or mischievous purposes. Several recent incidents of defaced Web sites between the Israeli and Muslim nations point to the clear potential for using the Internet as a powerful tool for manipulating information. While many instances of manipulation simply serve the cause of making a political or ideological statement and can be remedied rapidly, the more dangerous instances are those that go undetected. For instance the manipulation of financial data, military information, or functional infrastructure data.

- The threat of destruction of information or of critical infrastructure components can have gargantuan economic and national security consequences. Imagine if you will, a cyber attack on the Department of Transportation's Air Traffic Control Center resulting in all air traffic control capabilities for the entire eastern sector of the United States being shut down.

These possibilities are very real and must not be dismissed.

Specifically Communist China has recognized in their own documentation that they cannot match the United States militarily in a conventional way and that they will never be able to beat the U.S. in military might. However, they know that they can cause much more disruption with far less political consequences utilizing informational warfare because they clearly recognize how vulnerable the U.S. infrastructure truly is and what they can do to it by setting up the right techniques and mechanisms. The high-tech methodologies of conventional terrorists attacks will eventually make destructive attacks like the suicide style attack on the Navy's U.S.S. Cole in Yemen an obsolete methodology for carrying out their acts of terrorism. Cyber-terrorists factions of the future will not have to sacrifice the lives of their comrades via conventional attack methodologies simply to cause a comparatively minor disruption like the U.S.S Cole incident in the future. Now they can sit comfortably in front of a computer from half way around the world and access all of those aforementioned vulnerable systems to disrupt our entire economy and way of life. The traditional terrorist organizations have not really adopted this doctrine yet, although they are far more active in that arena now than ever before. Their current leadership didn't grow up with this technology so their preferred methodology of political and societal disruption is still being done by conventional means, such as blowing things up with explosives at the expense of a few of their comrades lives. When the technically savvy new generation of leadership in terrorist organizations and hostile nation states eventually move into positions of leadership, they will effect change of their attack doctrines and we will see far more coordinated cyber attacks on a much larger scale. Those attacks will have the potential to be much more disruptive and destructive to our society plus they will be able to do so without loss of live of their comrades and at far less economical expense. More "bang for the buck" so

to speak. It will also be much more difficult for the United States to track these individuals down in an effort to bring them to trial in International Court because they will not have to risk leaving any physical evidence behind for forensic study.

According to the Presidential Decision Directive (PDD) #63,

> "no later than 2003 the United States shall have achieved and shall maintain the ability to protect our Nation's critical infrastructures from acts that would significantly diminish the abilities of:
>
> - the federal government to perform essential national security missions and to ensure the general public and safety;
> - state and local governments to maintain order and to deliver minimum essential public services;
> - the private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial, and transportation services; and
> - any interruptions or manipulations of these critical functions must be brief, infrequent, manageable, geographically isolated, and minimally detrimental to the welfare of the United States."

Albeit that is a noble and worthy goal but I fear it is an unrealistic one simply due to the technical complexity, inherent costs, and magnitude of effort required to accomplish those goals in the time frame allotted. However, in the same breath, no matter how daunting the job may be we must try to accomplish exactly that. Our way of live could very well depend on it. For more information on Presidential Decision Directive #63 you can contact the Critical Infrastructure Assurance Office at (703) 696-9395 for copies of the White Paper on Critical Infrastructure Protection.
http://www.ojp.usdoj.gov/osldps/lib_pdd63.htm

In Conclusion:

We, the Information Systems Technical Experts in the private, academic and government sectors, are the now by default the Minutemen of the New Millennium because we have the collective knowledge and ability to become our Nation's Cyber Warriors in this new form of warfare. Our Nation's virtual digital borders are being attacked regularly and systematically in an effort to damage our very tangible and physical infrastructure that resides within our national borders. Our call to digital arms has been sounded. It is up to us to raise the standards and develop new methodologies in the science of Intrusion Detection and Protection. We need new tools as yet developed and new ideas that will ultimately help stem the tide of all of the aforementioned problems and issues that this new and extremely disruptive invention called the Internet has, and will continue to

bring. We need more effective ideas such as the DShield Project. DShield is, in effect, a Distributed Intrusion Detection System. It provides a platform for users of firewalls to share intrusion information. It is a free and open service and is an attempt to collect data about cracker / hacker activity from all over the Internet. This data will be cataloged and summarized and can then be used to discover trends in activity and prepare better firewall rules. Right now, the system is tailored to simple packet filters. As firewall systems that produce easy to parse packet filter logs are now available for most operating systems, this data can be submitted and used without much effort. Basically it is a form of distributed computing that can be a very powerful tool if properly managed, studied and supported. There's no telling where other new ideas and technologies, or ones like DShield, can lead. Nor what defensive and or offensive tools that could be developed from technological innovations of the future if we continue to work together and share our ideas. Until we all support innovative and effective ideas like this one, and others still yet to emerge, we will never advance the science required to establish the level of national security we need in order to successfully protect and defend our Nation's infrastructure. We must remember that in our line of work, paranoia is our friend.
http://www.dshield.org/intro.html

This is your unofficial call to digital arms! You are now more informed about the grave seriousness and astonishing magnitude of the threat to our Nation's critical infrastructure than the average citizen would ever really want to know about in the first place. Therefore, I emphatically urge you to get systems security trained and then get involved. The more Information Security trained Cyber Warriors we have fighting this current and future cyber-war, the better our chances of preserving our country's national security and way of life. Our cyber enemies will be better trained in the future on new and more effective digital methodologies for attacking our critical infrastructure, therefore we must get more organized and better trained as well in order to defend it. Become a Cyber Warrior. Our Nation and our way of life may very well depend on it in the not too distant future.

References:

Phoenix Health Systems. "HIPAA / Health Insurance Portability & Accountability Act (Public Law 104-191)." August 21, 1996 URL: http://www.hipaadvisory.com/regs/HIPAAprimer1.htm

Bridis, Ted and Buckman, Rebecca. "Microsoft hacked! Code stolen?" October 27, 2000. ZDNet News. URL: http://www.zdnet.com/zdnn/stories/news/0,4586,2645850,00.html

National Infrastructure Protection Center (NIPC). May 13, 2001. URL: http://www.nipc.gov/

Coffman, K. G. and Odlyzko, A. M. at AT&T Labs – Research. "Internet growth: Is there a ``Moore's Law" for data traffic?" July 11, 2000. URL: http://www.research.att.com/~amo/doc/internet.moore.pdf

Central Intelligence Agency. "Global Trends 2015:
A Dialogue About the Future With Non-government Experts." December 2000. URL:
http://www.cia.gov/cia/publications/globaltrends2015/index.html

Critical Infrastructure Assurance Office. Presidential Directive Decision #63. October
1997. URL: http://www.ojp.usdoj.gov/osldps/lib_pdd63.htm

Euclidian Consulting. Distributed Intrusion Detection System (Dshield.org) Introduction.
January 8, 2001. URL: http://www.dshield.org/intro.html