WISE
Washington Internships for Students of Engineering

Solving the Cyber Security Problem: The Role of the Department of Homeland Security

Jennifer Christensen

South Dakota School of Mines & Technology

August 2003

This report was submitted to the Institute of Electrical and Electronics Engineers, Inc. (IEEE) to fulfill the research requirements of the Washington Internships for Students of Engineering (WISE) program for the summer of 2003.

Table of Contents

About the Author

Jennifer Christensen is a junior double majoring in electrical engineering and mathematics at South Dakota School of Mines and Technology in Rapid City, SD. This paper is the result of ten weeks of research as part of the 2003 Washington Internships for Students of Engineering (WISE) program in Washington, DC. Her internship was sponsored by the Institute of Electrical and Electronics Engineers (IEEE).

About WISE

The Washington Internship for Students of Engineering (WISE) program is a ten week introduction to policy making for engineering students. Each year, twelve to sixteen junior and senior engineering students are selected to spend a summer in Washington learning about how technical decisions are made in government. The students visit various governmental and non-governmental organization representatives throughout the summer to gain a greater perspective on the operations of Washington. Additionally, each student is required to research and present a paper on a current policy issue related to engineering.

Acknowledgements

The author would like to acknowledge the IEEE for sponsoring her and for all of their support throughout the summer. Special thanks to Chris Brantley for being the best mentor around and a great teacher. Also, thanks to Dr. Jim Dennison, the Faculty-in-Residence for his help during the summer, as well as Allian Pratt for her coordination efforts. Finally, the author is grateful to the many people who took time out to meet and share information with her.

Introduction

Few experts would argue against the fact that cyber security will play a vital role in the future security of our nation and the American people. The problem lies in communicating and addressing the issue on a national level before it is too late. Prior to the attack on September 11th, experts had identified problems in our security measures. Sadly, it took an attack for the rest of the world to accept and act upon those notions.[1] Again we are faced with a similar situation. The experts are handing out warnings, and it is up to the government and the private sector to act upon those, or wait and face unknown consequences.

Vast amounts of information are available at the press of a button. The government and private sector are increasingly dependent upon computers and network systems. The increase in computer reliance should be accompanied by an increase in computer security needs and developments. This, however, is not happening at the same rate. While it is easy to increase computer usage, it is much more difficult and expensive to create new technologies to keep it secure. Especially for the Internet, a system created to share information, not hide it.

For all these reasons, cyber security has become a hot topic in government. The Department of Homeland Security has been targeted as the solution to our cyber security problems. As the protector of America's critical infrastructures, the Department has been assigned the task of helping to ensure that our computer networks and systems are also well protected. This job, however, is not as straightforward as it sounds. The computer infrastructures are much more complex and technologically sophisticated than bridges or ports. The Internet operates and functions far outside of the United States, and there is no way to simply build up a border and defend it. Unlike physical challenges, cyber security will require great amounts of technology and education for all computer users.

The DHS has just begun to tackle the numerous problems associated with cyber security. This paper will assess different areas of their involvement, and how others view government's progress. There are five major issues that will be addressed in this paper: assessing the cyber threat, the priority of cyber security in the DHS, defining the role of industry, raising public awareness, and research and development. Each of these topics is crucial to the success of the cyber security problem. Not all of them have straightforward answers. This paper will attempt to provide an overview of each issue, and why it should be addressed by the DHS.

---

[1] Paller, Alan. Testimony before the Subcommittee on Cyber security, Science, and Research & Development. Select Committee on Homeland Security. Oversight Hearing: *Overview of the Cyber Problem: A Nation Dependent and Dealing with Risk*. June 25, 2003. Available online at <

Overview: DHS Organization

The Department of Homeland Security (DHS) has been working tirelessly for the last year in order to realize a meaningful and successful organization. They transferred approximately 180,000 employees from numerous different agencies into the new department. Created by the Homeland Security Act of 2002 (Public Law 107-296), their mission is to protect the US from terrorist attacks by reducing vulnerabilities and to assist in recovery and minimize damage from these attacks. The Department is arranged into five main directorates: Border & Transportation Security; Emergency Preparedness & Response; Science & Technology; Information Analysis & Infrastructure Protection; and Management. The two directorates overseeing cyber issues are the Information Assurance and Infrastructure Protection (IAIP) and the Science and Technology (S&T).

The IAIP directorate, pursuant to P.L. 107-296, was formed from a merger of groups from different agencies. The consolidation was intended to create increased communication and progress. The transfers include the Critical Infrastructure Assurance Office (CIAO), the National Communications System (NCS), the National Infrastructure Protection Center (NIPC), the National Infrastructure Simulation and Analysis Center (NISAC), and the Federal Computer Incident Response Center (FedCIRC). Each of these groups transferred from different agencies where they performed various similar, yet independent, tasks. On June 6, 2003, the DHS introduced the National Cyber Security Division. The purpose of the division is to accomplish three main tasks: identifying risks and vulnerabilities as well as working to reduce them in government, overseeing a cyber security coordination project hub named the Cyber Security Tracking, Analysis & Response Center (CSTARC), and to help build cyber security programs to promote greater awareness of computer users.[2] The division is overseen by the Assistant Secretary of Homeland Security for Infrastructure Protection, Robert Liscouski. The position of the division director is vacant, and it is unclear how long it will be before they can fill the position.

The S&T directorate, not a part of the President's original plan for the DHS, was amended to the bills in congress in order to promote research and development within the new agency. The Directorate is headed by Under Secretary Dr. Charles McQueary, and is composed of several existing research agencies, along with responsible for creating some new groups to fill in the holes in order to meet the department's needs. The transfers include programs from the Department of Energy, the Department of Defense, and the Department of Agriculture, including the Advanced Scientific Computing Research program at Lawrence Livermore National Laboratory. Other programs in biological weapons and nuclear issues are the most heavily funded of the transferring organizations.

The Homeland Security Advanced Research Projects Agency (HSARPA) was created as part of the DHS S&T directorate. This research agency, formed as an equivalent to

[2] *National Cyber Security Division Press Release*. 6 June 2003. Available from <www.dhs.gov>

DARPA for the DHS, will have a myriad of uses. Most importantly, it will be a center of research devoted entirely to fulfilling the needs of the department. Some observers believe the HSARPA will have some operational differences from DARPA. The projects at DARPA are usually based on a 3-5 year program plan. The HSARPA should also have funding available for short-term solutions in emergencies or crises that require immediate action. Jane Alexander was recently appointed to fill the position as Director of the HSARPA. She has worked at DARPA and has experience managing programs and research projects.

1. Threat Assessment

A major problem in cyber security thus far is that there are so many unknowns. Without concrete numbers and statistics, it is hard to both understand and communicate the threat we are facing. The need for a serious assessment is extreme—without information regarding the types of cyber attacks, the perpetrators, and the possible consequences, it is much more difficult to know where to focus research and development efforts and how best to defend our critical infrastructures.

It appears the government has recognized the need for more information regarding the nature of the threat. They have assigned the DHS an assessment role. The IAIP directorate, specifically, is given the responsibility

> *To carry out comprehensive assessments of the vulnerabilities of the key resources and critical infrastructure of the United States, including the performance of risk assessments to determine the risks posed by particular types of terrorist attacks within the United States (including an assessment of the probability of success of such attacks and the feasibility and potential efficacy of various countermeasures to such attacks).*[3]

This role is assigned in order for them to create, based upon the results of the assessment, a list of priorities for development of homeland security protection. The vulnerabilities noted above should include those used in cyber attacks. What the DHS has done to complete this task is unclear, but the significance of their role is immense. It displays that the government is aware of the lack of a concerted effort to find and track the number of security incidents in computer networks.

In order to address these vulnerabilities and threats related to cyber security, it is essential to understand the concept. Cyber security, while different for every situation and network, is based around three basic tenets: confidentiality, integrity and availability.[4]

> **Confidentiality**: *A breach of confidentiality occurs when a person knowingly accesses a computer without authorization or exceeding authorized access.*

[3] Public Law 107-296

[4] *Computer Crime and Intellectual Property Section*. *Computer Intrusion Cases*. <http://www.cybercrime.gov/cccases.html> Accessed June 6, 2003.

Confidentiality is compromised when a hacker views or copies proprietary or private information, such as a credit card number or trade secret.

Integrity: *A breach of integrity occurs when a system or data has been accidentally or maliciously modified, altered, or destroyed without authorization. For example, viruses and worms alter source code in order to allow a hacker to gain unauthorized access to a computer.*

Availability: *A breach of availability occurs when an authorized user is prevented from timely, reliable access to data or a system. A popular example of this is a denial of service attack.*

Cyber security consists of tools, techniques or processes capable of protecting a system's information assets. While these tools and techniques vary from system to system, the overall idea behind cyber security remains constant: to be able to trust cyber systems and networks, and ensure the above three tenets are maintained.

The threat of cyber attacks grows everyday. It is difficult to get an accurate portrait of exactly how large the threat has grown, since most private companies are often unwilling to admit to system attacks and breaches, afraid that their consumers may loose confidence in them. However, it is possible to broadly identify the types of threats, risks and possible consequences attacks would have on the nation.

While the government has yet to complete a thorough assessment of cyber terrorism threats, there are other outside organizations working to document the problem. One important finding is that cyber attacks are increasing at a rapid rate. The Computer Emergency Response Team (CERT) at Carnegie Mellon, track the number of computer vulnerabilities and intrusions each year. These numbers show a dramatic increase in the last few years, seen in Fig. 1. Hackers are becoming increasingly prepared, organized, skilled and difficult to track.[5] Many hacking tools are easily accessible online, and require very knowledge from the user.[6] It is not surprising that attacks are increasing when they are cheap, easy and low risk to perform.

[5] Pethia, Richard D. Testimony before the Subcommittee on Cyber security, Science, and Research & Development. Select Committee on Homeland Security. Oversight Hearing: *Overview of the Cyber Problem: A Nation Dependent and Dealing with Risk*. June 25, 2003. Available online at <http://hsc.house.gov/files/Testimonty_Pethia.pdf >

[6] Pethia, written testimony.

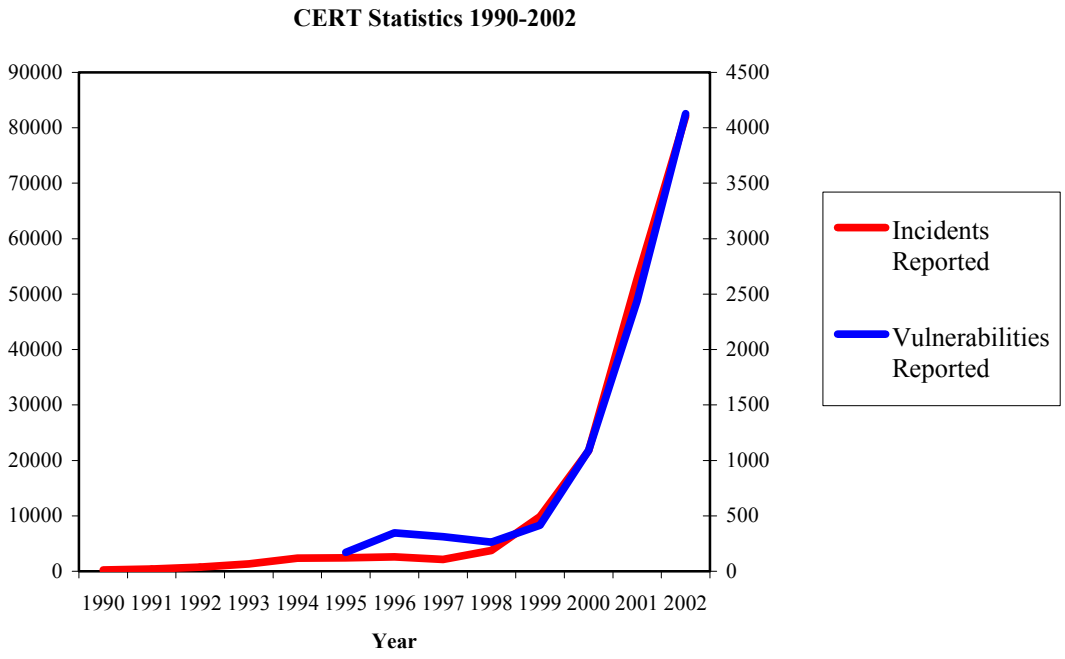

Figure 1. CERT Statistics on cyber incidents and vulnerabilities since 1990. Source: Carnegie-Mellon's CERT® Coordination Center

These statistics are alarming and display the need for greater investment in analysis and efforts to combat the problem. The exponential growth of incidents and vulnerabilities suggests that the number will continue to skyrocket in the future, resulting in greater damage costs. An accurate analysis will be the first step toward combating the growing problem of cyber attacks.

There are many different types of attacks that can be used to sabotage computer systems, the most common are listed below:

> *Worms*: A worm is a self-replicating virus that does not alter files but resides in active memory and duplicates itself. Worms use parts of an operating system that are automatic and usually invisible to the user. [7]
>
> *Viruses:* Coded like a worm, except it requires the user to do something in order for it to replicate.
>
> *Distributed Denial of Service (DDoS):* These attacks use multitudes of machines, unaware of their involvement, to overwhelm a specific target by flooding it with messages from all of the machines at once, making the target unable to function.

[7] From searchsecurity.com definitions

Insider Abuse of Net Access: Users with access to networks and systems use their knowledge to maliciously attack or disable a computer system an/or steal valuable data.

The different levels of sophistication in each category present a range of risks and consequences. Some attacks use more than one type to produce greater damage. For example, the recent Code Red worm included a denial of service payload.[8] The Slammer worm spread more rapidly than any before it. It infected 90% of vulnerable hosts in less than 10 minutes. It infected approximately 75,000 hosts in total. Fortunately, the Slammer did not contain a malicious payload, saving companies from serious information losses. It did cause serious problems for many, however. Bank of America's ATMs suffered errors and could not give out money, Continental Airlines cancelled flights due to problems with electronic check-in, and even Microsoft was unable to activate licenses for Windows XP users.

Allan Paller, of the SANS research institute, testified before congress at a hearing regarding cyber security.[9] Part of his testimony related his experiences with assessments of damage and costs. For the NIMDA worm, which was rampant for seven days following the attacks on September 11th, Paller interviewed numerous victims. Reported figures ranged from $300 to $700 of damage for each system. Totaling that up for 150,000 infected systems, the cost is around $75 million. The press, however, reported numbers ranging from $835 million to several billion dollars. These are not the only unreliable figures; many of the accounts of hackers and damages have been greatly exaggerated, or simply false. These facts demonstrate the need for a common protocol for estimating damages in order to make the figures more reliable and consistent. The government's involvement will make the data more trustworthy and open to the public.

Although cyber attacks have not produced any serious consequences on physical infrastructure yet, with increasing sophistication and organization they may become a greater threat in the future. Michael Vatis, Director of the Institute for Security Technology Studies at Dartmouth College testified that "the likelihood of cyber attacks against U.S. and allied information infrastructures is high."[10]

The FBI has identified what they believe are the threats to critical infrastructures:

- *Criminal Groups:* Groups of hackers who attack networks and systems for purposes of monetary gain.

- *Foreign Intelligence Services:* Use cyber attacks as a tool for espionage.

- *Hackers:* A common threat, hackers cause various types of damage, ranging from webpage defacements to denial of service attacks.

- *Hacktivists:* Hackers who are politically motivated.

[8] A payload is the eventual effect of a worm or virus
[9] Paller, written testimony.
[10] Vatis, written testimony.

- *Virus Writers:* Create malicious code to attack computers.

- *Insiders:* Disgruntled former or current employees with insider access to networks that allows them to cause system damage and/or steal data from their company.

- *Information Warfare:* A future possibility, cyber attacks from foreign military groups on our critical infrastructure; a serious threat to national security.

The 2003 CSI/FBI Computer Crime and Security Survey reported that of the 488 respondents, 82% regarded independent hackers as a likely source of attack, and 77% included disgruntled employees, both much higher than the other three categories: U.S. competitors, foreign corporations, and foreign governments.[11]

The National Security Agency (NSA) has affirmed that foreign governments have or are working to develop the abilities to attack others using computers. Not surprisingly, the probability of these attacks and the potential targets are unknown.

A problem facing those attempting to track cyber attacks is that the real threats are hard to distinguish from unsophisticated attacks due to the high level of network traffic. In other words, the number of hostile attackers is hidden by the noise produced by other non-threatening actions. This is yet another reason why an in depth analysis needs to be completed. It is hard to defend against an unknown threat, and as was seen by the surprise of September 11th, the magnitude of that threat may be greatly underestimated.

The President recommended $95 million in his FY2003 budget proposal for an infrastructure vulnerability and risk assessment in the IAIP. The House Appropriations Committee countered by allocating a little over $84 million. The Committee commented that it would like to see a greater number of cyber security intelligence analysts in the department, and directed the DHS to provide a program plan for the risk analysis and assessment by December 15, 2003.

There is a difference between analyzing threats and identifying vulnerabilities. The focus of the government should be to find a balance between the two types of activity. It will be very difficult to determine the threats from a global perspective, but such an analysis will help determine who is perpetrating the attacks, making likely targets easier to predict and secure. Finding vulnerabilities may not be as much of the government's job. Securing government systems should be a priority, and to do so, vulnerabilities must be identified.

---

[11] Only 92% of the 488 respondents of the survey submitted a response to this particular question. The other three categories measured in at 40%, 25% and 28%, respectively. These do not add to 100 since respondents were able to choose more than one source of attack.
2003 CSI/FBI Computer Crime and Security Survey. Computer Security Institute. 2003. Available online from <www.csi.org >.

The best way to secure our systems is to focus on the vulnerabilities rather than attempt to stop the attackers. There are too many attackers and threats from around the globe to be able to catch all the attackers, but if the government is able to secure their own systems from known vulnerabilities, and continue to protect themselves by using smart practices and updating security measures, the risk will be significantly reduced. To do so, an extensive and thorough assessment of vulnerabilities is necessary.

2. Prioritizing Cyber security at the DHS

The DHS is committed to protecting the United States from terrorist attacks. The job is much too big for this organization to tackle all at once, so they are required to prioritize, as is the government, what is most critical, and of greatest need. To figure out where cyber security lies in the big picture, it is necessary to look more in depth at the threats we are facing, as well as our vulnerabilities to serious attack. The government's priorities thus far can be seen through different areas of the organization and previous government actions in this area.

Without a serious assessment of the risks the nation faces from terrorist attacks (as discussed in part 1), it is difficult to prioritize the steps the DHS should take to combat these threats. There has been a great deal of spending and focus on first responders and other responses to major attacks, like the one on September 11th. This is natural, given that America has not seen any cyber attacks that would even come close to the destruction and cost of that attack. There are reasons to consider the threat of cyber attacks as well.

The importance of cyber security in homeland security is visible through the many different areas of American lives that it could potentially affect. There are different definitions of "critical infrastructures," but the following is a list of those most commonly referred to: telecommunications, power distribution, water supply, public health services, national defense, law enforcement, government services, and emergency services. If a cyber attack chose one of these areas as the target, there could be serious consequences for the nation. The extent of the damage, however, is a matter of debate. While some experts claim that some critical infrastructures are more resilient than others, and that their disruptions would be less detrimental to national security or to the economy, others see the potential risk in a different light.

James Lewis of the Center for Strategic and International Studies (CSIS) has argued that physical infrastructures are less vulnerable to cyber attacks than computer networks.[12] This is due to the overlaps and redundancies throughout the systems. These produce more difficult targets for hackers since it would take a greater number of attacks performed simultaneously to seriously affect the systems. Lewis also notes that critical infrastructures suffer from disruptions on a daily basis: power outages for several hours, air traffic delays and water system failures. While often inconvenient, none of these cause panic or serious consequences. For example, a recent survey showed that power

[12] Lewis, James A. Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. Center for Strategic and International Studies. December 2003. Available online from http://www.csis.com

companies are main targets for cyber attacks. Seventy percent of companies surveyed had "suffered a severe attack" in the first half of 2002.[13] While the power system is a popular target, the complexity and redundancy of the electric grid makes it extremely difficult to create a power outage. It would take require finding the vulnerabilities in numerous systems and attacking them simultaneously. Even with a number of hackers working together, it would not be an easy task, and would likely result in a few hours of disruption at the most. Not surprisingly, the number of blackouts in the US caused by cyber attacks is zero.

There are a few cases of cyber attacks having serious physical consequences. One such case took place in Australia in 2001 when a water facility was attacked by Vitek Boden, who had previously worked as a consultant for the project. Boden's successful attempt to access the system, his 45th try, enabled him to release nearly one million liters of sewage into the river and coastal waters. The result was black water, a horrible stench, and the loss of some marine life. While this incident was perpetrated by a disgruntled individual, not a terrorist group, many claim it demonstrated the possibility of cyber attacks on public utilities and critical infrastructures to cause damage.

The DHS insists that cyber security is a serious concern and, according to Tom Ridge, "we will pay as much attention to the Internet as we do physical." The evidence of their efforts so far reflects that it has been made a priority in many acts and speeches, but actual changes are still to come. The first acts of the Department were oriented toward securing physical sites, and testing the response systems. Despite this, it is clear that the DHS and the executive branch have cyber on their minds. "Cyber terrorism" became a concern during the recent war on Iraq, and the possibility of "an electronic pearl harbor" was touted. Cyber terrorism is defined as "the use of cyber tools to shut down critical national infrastructures (such as energy, transportation or government operations) for the purpose of coercing or intimidating a government or civilian population." [14]

Many of the concerns regarding cyber terrorism were perpetuated by the efforts of Richard Clarke, former special advisor to the President on cyber security. His influence in the government and nation to raise concerns about cyber security is immeasurable. In an interview with ComputerNews, Clarke stated:

> *Before Sept. 11, [al-Qaeda] was interested in killing as many people as possible. After Sept. 11, [Osama bin Laden] starts talking about destroying the American economy. And he starts to talk about going after the economic infrastructure of the United States. You could drive around a lot of truck bombs and really not do a lot of damage to the economic infrastructure because it's so diverse and dispersed. But if you do it in cyberspace, you might have the ability to hit the entire financial services network simultaneously.*

---

[13] Higgins, Mark, Ed. *Riptech Internet Security Threat Report.* Available online at http://www.securitystats.com/reports/Riptech-Internet_Security_Threat_Report_vII.20020708.pdf

[14] J. T. Caruso, deputy executive assistant director, Counterterrorism/Counterintelligence, FBI in March 21, 2002, testimony before House Subcommittee on National Security, Veterans Affairs and International Relations

Other experts in computer security are baffled by what they consider "hype" put forth from the government. Many believe that cyber terrorism is not a serious risk, and the government's interest in the area is overdone. Many associate Richard Clarke with this hype.

> *Cyberterrorism merges two spheres--terrorism and technology--that most lawmakers and senior administration officials don't fully understand and therefore tend to fear, making them likelier to accede to any measure, if only out of self-preservation. Just as tellingly, many are eager to exploit this ignorance. Numerous technology companies, still reeling from the collapse of the tech bubble, have recast themselves as innovators crucial to national security and boosted their Washington presence in an effort to attract federal dollars.*[15]

Whether or not the threat of cyber terrorism is real, cyber security remains a major issue. These are the areas that need to be addressed, but it is unclear where the government will focus efforts on the subject. The DHS will be involved, and it is their mission to protect the nation from terrorist attacks, but protection of our infrastructure is the critical element, not the attacker's origin or motive.

The organization of the Department reveals some weaknesses towards cyber security. First, there is no high level group dealing purely with cyber risks. The task has been assigned to the IAIP directorate, which also deals with intelligence information on all different types of attack. The consolidation of several cyber-oriented groups within the department displays concern for cyber security within the directorate, but low funding and other problems may inhibit their abilities to make serious changes.

One problem is smoothly transitioning to the DHS and staffing the agency. The IAIP directorate Under Secretary, Frank Libutti, was only sworn in last June. One staffing concern is the FBI's NIPC division transfer. The FBI created a special cyber crime division during a reorganization in July 2002. Before the transfer of the NIPC to the DHS, approximately one-third of the employees moved from the NIPC to the cyber crime division. Of the remaining two-thirds, many found other jobs within the FBI, resulting in approximately one-third to one-half of the possible employees actually making the transfer. This, unfortunately, leaves the developing IAIP with around 200 jobs to fill. There is an additional challenge to overcome, however. Since the DHS was developed as a consolidation of many preformed groups, it is not easy to hire new employees. And while there is a lack of leadership in the directorate, it is likely that fewer top candidates will be attracted to the positions.

On June 6, 2003, Secretary Ridge announced the creation of a new National Cyber Security Division within the DHS. The Division is part of the IAIP directorate, and has many responsibilities. This action displayed the DHS' commitment to addressing cyber

---

[15] Verton, Dan. "Cyberdefense Plan Gets Mixed Reviews" Computer World. 23 September 2002. Online <http://www.computerworld.com/securitytopics/security/ story/0,10801,74449,00.html> Accessed 22 July 2003.

security needs, but did not have a great effect otherwise since the groups were already slowly being assembled, and no director has been named. There have already been outcries from the private sector that the government is not taking cyber security seriously. While the division may seem like a step in the right direction, to many industry members it is not nearly enough. The division is placed, essentially, in the "third tier" of the DHS. The low status of the group will give the director much less influence than the former position of Richard Clarke, who recently retired from service. The responsibility of cyber security, and potential liability, however, is enormous. It is unlikely that a highly qualified candidate will be interested in taking a position with so much responsibility that lacks the appropriate corresponding authority. On the other hand, the division has added some much needed structure to the IAIP, where many were concerned with how the different groups would be coordinated and how they would interact with one another.

In the DHS, Under Secretary McQueary stated that the S&T directorate would be addressing concerns through focused portfolios.[16] Cyber security was addressed in two of the eleven portfolios: the threat and vulnerability, testing and assessment portfolio and the critical infrastructure protection portfolio. Within the first there was "extensive research and development activities in the area of cyber security, addressing areas not currently addressed elsewhere in the federal government." Specifically, insider threats were given as an example of an area where new technologies are needed. The second portfolio addresses the protection of physical infrastructure, but the main goal is to formulate a way to evaluate and prioritize different strategies and to assess possible attacks and consequences.

Funding of cyber security efforts has not been as substantial as that of other areas of the DHS. The President recommended $829 million to the IAIP in his budget, but the House Appropriations Committee recommended only $776 million. Funding issues are discussed later in the research and development area (see page 21).

Other governmental agencies are prioritizing cyber security. The Department of Defense, in particular, is extremely careful to guard their systems by separating them from the Internet as well as the Pentagon's network. New software must be tested for security by the National Security Agency. The Air Forces' Chief Information Officer, (CIO), John Gilligan, stated that "Terrorists could not gain control of our spacecraft, nuclear weapons, or any other type of high-consequence asset." Even if cyber security responsibilities are given to the DHS, other agencies such as the DoD , will have to continue to do their part to keep systems safe from intrusion.

The priority of cyber security in the Department of Homeland Security is arguably too high or too low, depending on your point of view. Industry and researchers argue for more funding for research and more government action. Government is focusing on physical and biological threats and protecting our borders and physical targets monetarily, but they have also given a lot of attention to the new cyber activities.

---

[16] McQueary, Dr. Charles E. Testimony before the Subcommittee on Cyber security, Science, and Research & Development. Select Committee on Homeland Security. May 21, 2003. Available online at <>

Whether or not this is warranted is hard to determine. Until a thorough assessment and analysis of the risks and possible consequences is complete, it is difficult to compare one area of critical infrastructure to another. Cyber attacks and vulnerabilities will continue to increase at an alarming rate if something is not done to prevent these. Making sure that as we become more dependent upon computers, security measures also increase is definitely an area of concern. The DHS must continue to assess the threat and take action to minimize the risks of attack, or it may become one of our greatest vulnerabilities.

3. Defining Industry's role

According to Andy Purdy, the S&T directorate's cyber security advisor, input from industry is a top priority.[17] Government's limited resources and the large amounts of work done by the private sector make a successful relationship between the public and private sectors a crucial part of development of cyber technologies and cyber security awareness. The more information sharing between the two, the faster new technologies can be produced and alerts given to computer users in order to stop cyber attacks.

The DHS will need to clearly define the role of industry in relation to government and establish trust between the two groups. The goals of industry and government are often very different, but in this case, the protection of our critical infrastructures can be made a unified effort. The creators of the DHS incorporated this idea into the legislation:

> *To request additional information from other agencies of the Federal Government, State and local government agencies, and the private sector relating to threats of terrorism in the United States, or relating to other areas of responsibility assigned by the Secretary, including the entry into cooperative agreements through the Secretary to obtain such information.*[18]

The role of industry is still undefined. There is definitely a lot of movement towards coordinating efforts between government and industry, but how far should government go? 80%-85% of our critical infrastructures are privately owned. How much can the government do to protect the nation from cyber attacks, and how much responsibility should be placed on the private sector?

Currently, there are very few standards or incentives for industry to increase its role in protecting computer systems aside from simply protecting their systems from business disruptions. Security is an expensive job, and rarely produces outcomes that are profitable. However, this may change as security breaches become more expensive risks and companies determine financial benefits from security. This is likely to happen since statistics show that the number of attacks and the level of damage are both increasing.

System administrators are overwhelmed by security products, but under funded. This is a serious problem that relates back to profitability. Executives are reluctant to spend

---

[17] Hasson, Judy. *DHS Center to focus on security research.* Federal Computer Week. 19 March 2003. Available online at <http://www.fcw.com/fcw/articles/2003/0519/news-security-05-19-03.asp>
[18] P.L. 107-296

money on security, making in far more difficult for security products to be bought and put into place. The majority of attacks on computers are upon known vulnerabilities. The problem exists in patching and fixing vulnerabilities in a timely fashion. It seems like an easy problem to solve, but there are no products or systems available with automatic patch installation, or other security help.

President Bush released the National Strategy to Secure Cyberspace this February. In it, five priorities are addressed.[19] The primary focus of the strategy was to help secure the nation's critical infrastructures from possible terrorist attacks. The greatest responsibility was placed on large enterprises and critical sectors/infrastructures, both of which played a role in all five priorities.[20]

The strategy has been both praised and criticized. While it displayed that the government was making cyber security an issue and raising awareness, it consisted purely of recommendations and suggestions—a "hands-off" approach. Critics argue that this plan will not solve the cyber security problems, it is only another in a large pile of similar reports. Preliminary copies of the Strategy included more recommendations on wireless communications, and suggestions that ISPs provide their users with personal firewalls, both of which were removed when industry protested. This shows the weakness of the paper. Some believe the preliminary drafts were intended to test the initiative to determine if there was enough political support to go through with serious recommendations. The released draft seems to indicate a negative response, proving that more work must be done to make cyber security a priority in the private sector. The lack of serious regulations also indicated that government is depending upon industry to initiate its own standards for security measures. Some companies have responded to the Strategy positively, and are working to implement the suggestions given while others have more or less shrugged it off.

The private sector plays a crucial part in the research and development as well as the implementation of new technologies and securities. Thus far, it has not been to their advantage to invest in these types of securities due to the lack of profitability. Businesses are reluctant to invest large amounts of money in products that will still not make their systems secure, especially when they have not seen quantified amounts of risk. The government is concerned with this problem, and has begun to look at possible solutions/incentives.

A familiar solution to many governmental problems is regulation. Several experts[21] referred to the use of seatbelts as a comparable problem: Government mandated that the automotive industry put seatbelts into cars, and everyone benefited. If the government mandated using security measures in private sector computer use, there would likely be fringe benefits to all computer users. This, however, would not be a popular solution for

[19] The five priorities outlined are: 1) A National Cyberspace Security Response System, 2) A National Cyberspace Security Threat and Vulnerability Reduction Program, 3) A National Cyberspace Security Awareness and Training Program, 4) Securing Governments' Cyberspace, and 5) National Security and International Cyberspace Security Cooperation.
[20] *National Strategy to Secure Cyberspace.* Available from <http://www.whitehouse.gov/pcipb/>
[21] From Keith Schwalm interview and Schneier testimony

industry, since that would require a greater expenditure with little return. Also, depending on your political stance, it may overstep the bounds of government's role.

Industry is also looking into insurance against cyber attacks. If this happens, there will have to be standards drawn up by insurance companies, which may help raise the level of security in general, as well as protecting companies from financial losses resulting from a serious attack. The option of insurance will only be worthwhile if industry recognizes the growing cost of cyber attacks. Another factor, which would help influence the private sector to invest more heavily in security products, is liability. If software companies are held liable for a set of security standards, overall quality of products will improve.

To obtain the private sector's opinion, members of industry were asked to testify regarding what the government's priorities in cyber security should be. Before the Select Committee on Homeland Security, executives from Sun Microsystems, AT&T, AOL, Microsoft, Dell and Equinox, Inc. related what they believe are the major problems involving cyber security and what they are doing to improve the situation. Several also submitted their ideas concerning the government's contribution to securing our systems. All supported additional funding for R&D, many mentioned increased cooperation among law enforcement and industry to catch and prosecute hackers more effectively. AT&T specifically argued against the government implementing a standard of security which they claimed would be at an "arbitrary level." Microsoft stressed the importance of the government leading the way into more secure systems by setting an example and using procurement to affect change.

Procurement is another possible government action. Other testimonies before the committee included Dr. Shankar Sastry's comments on cyber security. Dr. Sastry suggested that the S&T, IAIP and Borders directorates all use procurement to secure their own systems in order to "jump start" the industry efforts.[22]

Eugene Spafford, of Purdue University, has similar ideals as much of the industry leaders. He identified securing critical computing infrastructures on both the governmental and the civil sector as what should be the number one priority of the government's cyber security efforts. His reasons for encouraging funding for R&D were based on uncertainty regarding the private sector's willingness to spend money on cyber security without some sort of incentive.[23] This is a common theme from experts outside of industry. Many believe it will require some initiative from the government to get the companies to start investing seriously in security.

The director of the NIPC, Michael Vatis, testified before the Senate Judiciary Committee that our success in battling cyber crime depends mostly upon cooperation from the private sector. The private sector is the victim in the majority of cyber attacks, so in

[22] Sastry, Shankar. Testimony before the Subcommittee on Cyber security, Science, and Research & Development. Select Committee on Homeland Security. 22 July 2003.

[23] Spafford, Eugene. Professor of Computer Sciences at Purdue University. Director, Center for Education and Research in Information Assurance and Security (CERIAS). Personal email correspondence.

order to find and prosecute perpetrators, companies must share information with the government and willingly aid investigators.

The NIPC has had some success already working with industry. They began a program with the North American Electrical Reliability Council (NERC) to provide the NIPC almost real time reports of cyber problems at electric and power companies. The benefit to NERC is feedback and analyses of incidents from NIPC, who also issues warnings if they believe it necessary. This program shows the advantages derived from open communication between government entities and the private sector.

Other programs are beginning to form among industry groups as well. Microsoft, AMD, Intel, IBM, and Hewlett-Packard came together early this year to form the Trust Computing Group (TCG). This not-for-profit assembly was created to help promote and set open-standards for cyber security technologies. There are other organizations currently forming to facilitate a higher level of communication between corporations, as well as the government. The Information Technology—Information Sharing and Analysis Center (IT-ISAC) is supported by industry members and promotes sharing regarding vulnerabilities and attacks.[24] These groups are a step in the right direction. The more industry takes on itself, the more likely it will be for the whole to improve. Government standards are often too rigid for smaller companies and are not flexible enough for an ever-changing environment, like that of technology.

Howard Schmidt tackled the question of legislation on security standards by stating: "They're good at a lot of things but when it comes to writing laws about technology--how do you write a law about technology? Do you write a law that says you must use common sense; do you write a law that says you must turn on your firewall? It's just not practical…"[25] He pinpoints the primary problem relating to security: government cannot produce laws and standards which will be effective in the long term. This predicament makes industry involvement essential. Positive changes will be more prevalent with industry support. The government is not immobile, however. Their role should be as a coordinator and consumer. The needs of the government in information security should serve as a starting point for industry standards, and hopefully in the future, that will expand to serve the entire nation.

4. Raising Public Awareness

> *Each American who depends on cyberspace, the network of information networks, must secure the part that they own or for which they are responsible*.
> –National Strategy to Secure Cyberspace

The need to inform Americans and all computer users about the threat of cyber attacks is great. Computer systems are so reliant upon another and interconnected that truly, the

[24] Reitinger, Philip. Testimony before the Subcommittee on Cybersecurity, Science, and Research and Development. Select Committee on Homeland Security. 15 July 2003.
[25] Savage, Marcia. *CRN Interview: eBay Security Chief Howard Schmidt*. CRN. 17 June 2003. Available online at http://crn.channelsuperserach.com/news/crn/42709.asp

chain is only as strong as the weakest link. If there is only one person not safeguarding his/her computer, the whole network may be in jeopardy. That is why it is essential that the public is aware of what types of risks they may be taking.

Why the role should be given to the government is a different question. The government has the broad outreach abilities that other industry members do not have. While the government may not be responsible for all of the work, forming the coalition and setting goals for public awareness is something they are capable of doing, similar to their involvement with industry. The DHS was given the charge of undertaking this project in its new National Cyber Security Division:

> *Create, in coordination with other appropriate agencies, cyber security awareness and education programs and partnerships with consumers, businesses, governments, academia, and international communities.*[26]

The Division is still underway, so it is unlikely that too much has changed. But the private sector has been concerned with this issue and working on it for quite some time. There are several main problems that are influencing industry to get involved in cyber security awareness.

First, the problem is not well understood. Few computer users understand the risks and vulnerabilities that are inherent to their systems. Computers have become much easier to use and access, but education and information about security risks and possible threats remain greatly unspoken. This is not always the user's fault, as many companies are reluctant to share weaknesses and problems in their systems with the public.

Eugene Spafford, of Purdue University, testified regarding the threats of cyber attacks. In his testimony, Dr. Spafford noted that personal computers are currently used far beyond the purposes for which they were originally intended. This includes maintaining defense information and computer networks. The problem is that their systems are often unprotected, leaving them vulnerable to viruses which then spread to other systems on the network. There is also a huge user population, many of whom are unaware of the potential consequences of their actions.[27]

Other organizations have noticed a similar problem. The organizers of Infosecurity Europe 2003, a huge security exposition, noted that approximately 90% of office workers were willing to reveal their passwords to a questioner at a station in London. The number is up from 65% in 2002. This survey, while not conducted in America, reveals the possible vulnerabilities that uninformed employees create. The article addresses greater awareness and states:

> *What strikes you is that in corporate-land and in the community, we are failing our citizens to our own detriment. There is a woeful lack of awareness campaigns*

[26] National Cyber Security Division Press Release. Available from www.dhs.gov. 6 June 2003.
[27] Spafford, written testimony.

> *in information security programs. People need constant reminders. People need to know what the threats look like.*[28]

Other governmental officials have also begun to emphasis the need for greater public awareness. The President's National Strategy to Secure Cyberspace named one of its five priorities "A National Cyber Security Awareness and Training Program." The Strategy details the numerous vulnerabilities from awareness issues which can easily be ramified through training. The four main actions outlined are: to encourage a national awareness program for all Americans, provide training and education, increase the efficiency of training programs, and to promote the private sector's involvement.[29]

Howard Schmidt, Richard Clarke's former second in command and currently eBay's security chief, also discusses awareness in an interview. He states:

> *The third piece is training. We teach people how to drive, but we don't do a good job teaching people about cybersecurity. Cable modems, DSLs - wonderful technology but we're just beginning to see the service providers, when they install, give you a pamphlet that says, here's learning about personal firewall, here's antivirus links.*[30]

The attack by Vitek Boden on the Australian water utility can be mentioned in this section as well. The fact that 44 attempted attacks on the system went unnoticed speaks loudly about the need for greater awareness and training.

The DHS must promote greater awareness of cyber security. This will help protect our infrastructures and all of our systems. While industry may be able to help in this area, and should be responsible for creating and implementing their own training programs, the DHS should be responsible for doing the same among government agencies, with their help. It can also help home users by creating a national campaign to encourage and inform them of the risks they face. These actions may result in a consumer push for better security products, which would force industry to comply and, in doing so, continue to raise the level of cyber security throughout the nation.

5. Research and Development

The last issue concerning cyber security in the DHS is research and development. The scope of this issue is large enough to warrant a separate paper entirely, so this section will merely touch on some key aspects. The biggest challenge facing the DHS cyber security efforts is a lack of funding to complete the mission it has been assigned. The transition is nearing completion, the funding is now necessary to more forward and begin to tackle

---

[28] McIntosh, John. *Security is a People Problem—Right?* Bloor Research. 6 May 2003. Available online at < http://www.it-analysis.com/article.php?articleid=3765>

[29] *National Strategy to Secure Cyberspace.* Available from <http://www.whitehouse.gov/pcipb/>

[30] Savage, Marcia. *CRN Interview: eBay Security Chief Howard Schmidt.* CRN. 17 June 2003. Available online at http://crn.channelsuperserach.com/news/crn/42709.asp

some of their most pressing needs. A huge part of the R&D efforts will be focused towards implementation of technology, desperately needed to help move research and ideas into products.

The DHS could become one of the top federal R&D funding agencies, given the amount requested in the president's FY 2004 budget. The request gave the Department 1.0 billion dollars in funding. While the department was created mainly through transfers and of other programs from a range of different agencies, some of the R&D will be coordinated through major new initiatives, such as the HSARPA. 80% of the R&D funding is in the S&T directorate.

The IAIP Directorate will have to rely upon the S&T directorate for key research support, since a mere $5 million of their $829 million budget request is dedicated to research and development. However, the S&T directorate has allocated approximately $18 million of their $803 million towards cyber security. The result of the $18 million may be one or two good research projects, not enough to make a large change. The initiatives are now focusing on getting involvement from industry as well, and coordinating their efforts so that the government becomes merely a contributor to the larger pot of R&D investments.

The HSARPA was included in the president's FY 2004 budget with a start up budget of around $350 million.

The DHS is not alone, many other agencies are also involved in cyber security research and development. The majority of work in this area has previously been accomplished by DARPA. Alliances with several other organizations, including the National Science Foundation (NSF) and the National Institute of Standards and Technology (NIST), helped further this research.

The Cyber Security Research and Development Act (P.L. 107-305) authorized much greater funding to NSF and NIST. The Act, signed into law on November 27, 2002, gave nearly $900 million dollars to further research into cyber security over the next five years. The goals of the legislation are: to improve basic research; to encourage partnerships between academia and industry; and to generate a new cyber security workforce by investing in fellowships and scholarships. The NSF is authorized a total of $568 million over the next five years for research grants, to create centers for multidisciplinary research, and grants for undergraduate, graduate, and doctoral education programs. NIST is authorized $310 million over the same five years. This money is to create more partnerships between the private and public sectors, as well as again encourage education through fellowships. There are also provisions for NIST to conduct analyses of threats to the cyber world, as well as a two-year study at the National Academy of Science (NAS). This authorization displays some of the priorities that have been set in the Science Committee and the legislative branch: greater research and educational investments, along with a commitment to work with the private sector.

> *It's not as if I worry tomorrow that the entire Internet is going to go down. None of those things will happen, but we should not be susceptible to even short interruptions because of things that are within our capacity to fix. The processes*

are there, the technology is there, the understanding is there, ***we just have to implement it****.* –Howard Schmidt[31]

Perhaps most important of the DHS' role in cyber security will be the implementation of technology. They have emphasized that they will not simply be researching, but they will be developing technologies to be applied to systems as soon as complete. Many university research labs and other cyber security centers have created innovative technologies, but there is a void when it comes to implementation. This gap between basic research and products has caused problems in all areas of research, a problem the DHS is keen to fix.

As previously mentioned, the majority of the efforts in the S&T directorate will be devoted to implementation of technologies. This is consistent with their budget, which invests most in development, and a mere 10 percent for basic and applied research. The organization and communication between the IAIP and the S&T will also be crucial.

Looking back on the role of industry, this is another area where they could have a tremendous amount of impact. Creating public-private partnerships to address the implementation of new technologies will make changes happen much more rapidly. These partnerships are cooperative understandings between different areas of the security market (academia, private companies, and the government) which help bring new ideas and products rapidly into use.

The research that is done in the DHS will no doubt make a positive impact on cyber security. The low funding for these initiatives means that they should work to further their relationship with industry and universities to produce more for the money. Coordination to prevent overlap and share new ideas will be the key to faster results. Implementation will be the DHS' greatest asset. If they can move ideas into products smoothly and quickly, cyber security may see great improvements. The biggest problem is using the technology, and getting it installed, as we see with patches which go for weeks without being installed. Protecting our critical infrastructures will take new technologies, and new products. If the DHS can provide both in a short period of time, we may eventually be able to step ahead of the hackers and their technologies.

[31] Savage, Marcia. *CRN Interview: eBay Security Chief Howard Schmidt*. CRN. 17 June 2003. Available online at http://crn.channelsuperserach.com/news/crn/42709.asp

Conclusion

To secure our Nation's critical infrastructure from terrorist attacks, the Department of Homeland Security was created. In it, a critical part of that security effort was addressed: cyber security. The need for a center of coordination and progress was urgent, and the DHS is working to fill that gap. The main areas they now need to focus on have been outlined in this paper: assessing, prioritizing, defining industry's role, raising public awareness, and supporting research and development.

Each area has separate goals, but they intertwine to form a basis for good security practices in government and as a nation. These issues are only the beginning in what may become a critical area for protecting our nation's assets and information. The role of the computer is continually changing, as we become more dependent upon technology in all aspects of our lives. So, therefore, must the technology change in order to keep pace and continue to protect us from those with malicious intentions. Assessing where we stand today will serve as the base to move forward from. Raising awareness and defining industry's role will help move these changes forward, as will new technologies from research. Prioritizing cyber security will help aid all of these efforts by securing additional funding and support for DHS initiatives.

Cyber security is in good hands. The DHS is committed towards making our nation safer, and while it will require effort from all sectors in both the government and public, it is a problem that is being addressed, and positive changes will continue to be made.

Reference

2003 CSI/FBI Computer Crime and Security Survey. Computer Security Institute. Available online from <www.csi.org>

AAAS Report XXVIII: Research and Development FY 2004. Intersociety Working Group, American Association for the Advancement of Science. 2003.

Bush, George W. *National Strategy to Secure Cyberspace.* Available from <http://www.whitehouse.gov/pcipb/>

Higgins, Mark, Ed. *Riptech Internet Security Threat Report.* Available online at http://www.securitystats.com/reports/Riptech-Internet_Security_Threat_Report_vII.20020708.pdf

Koizumi, Kei. Director, Budget and Policy Program. American Association for the Advancement of Science. Phone Interview. June 24, 2003.

Lewis, James A. *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. Center for Strategic and International Studies*. December 2002. Available online at http://www.csis.org/tech/0211_lewis.pdf

Lewis, James A. Cyber *Attacks: Missing in Action*. April 2003. Available online at <http://www.csis.org/tech/0403_cyberterror.pdf >

McIntosh, John. *Security is a People Problem—Right?* Bloor Research. 6 May 2003. Available online at < http://www.it-analysis.com/article.php?articleid=3765>

McQueary, Dr. Charles E. Testimony before the Subcommittee on Cyber security, Science, and Research & Development. Select Committee on Homeland Security. May 21, 2003.

National Cyber Security Division Press Release. 6 June 2003. Available from <www.dhs.gov>

Paller, Alan. Testimony before the Subcommittee on Cyber security, Science, and Research & Development. Select Committee on Homeland Security. Oversight Hearing: *Overview of the Cyber Problem: A Nation Dependent and Dealing with Risk*. June 25, 2003. Available online at http://hsc.house.gov/files/Testimony_Paller.pdf

Pethia, Richard D. Testimony before the Subcommittee on Cyber security, Science, and Research & Development. Select Committee on Homeland Security. Oversight Hearing: *Overview of the Cyber Problem: A Nation Dependent and Dealing with Risk*. June 25, 2003. Available online at http://hsc.house.gov/files/Testimonty_Pethia.pdf

Reitinger, Philip. Testimony before the Subcommittee on Cybersecurity, Science, and Research and Development. Select Committee on Homeland Security. 15 July 2003.

Roberts, Paul. "NIPC Leadership, Protocol Questioned." 27 February 2003. Available online at <http://www.infoworld.com/article/03/02/27/Hnnpic_1.html>

Sastry, Shankar. Testimony before the Subcommittee on Cyber security, Science, and Research & Development. Select Committee on Homeland Security. 22 July 2003.

Savage, Marcia. *CRN Interview: eBay Security Chief Howard Schmidt*. CRN. 17 June 2003. Available online at http://crn.channelsuperserach.com/news/crn/42709.asp

Schneier, Bruce. Testimony before the Subcommittee on Cyber security, Science, and Research & Development. Select Committee on Homeland Security. Oversight Hearing: June 25, 2003. Available online at http://hsc.house.gov/files/Testimony_Schneier.pdf

Schwalm, Keith. Department of Homeland Security. Science and Technology Directorate, Secret Service. Personal Interview. July 9, 2003.

Spafford, Eugene. Professor of Computer Sciences at Purdue University. Director, Center for Education and Research in Information Assurance and Security (CERIAS). Personal email correspondence.

Suski, Greg. Department of Homeland Security. Science and Technology Directorate, Technical Intelligence. Personal Interview. June 27, 2003.

United States General Accounting Office. *Progress Made, But Challenges Remain to Protect Federal Systems and the Nation's Critical Infrastructures* GAO Report GAO-03-564T. 8 April 2003. Online: www.gao.gov/cgi-bin/getrpt?GAO-03-564T

Vatis, Michael A. *Cyber Terrorism: The State of U.S. Preparedness*. Testimony before the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations. House Committee on Government Reform. Sept 26, 2001.

Verton, Dan. "Cyberdefense Plan Gets Mixed Reviews" Computer World. 23 September 2002. Available online at <http://www.computerworld.com/securitytopics/security/story/0,10801,74449,00.html> Accessed 22 July 2003.

Wilson, Jim and Joe Czika. House Science Committee. Minority Staff. Personal Interview. June 2003.