Global Information Assurance Certification Paper

The Impact of Homeland Security Initiatives on Information Assurance

Randall Owen
GSEC Practical Assignment
Version 1.4b, Option 1
April 18, 2003

Abstract

There is no doubt that terrorism and homeland security have taken top priority in governmental policy and affairs since the terrorist attacks of September 11, 2001. We see examples of this just recently with the release of "The National Strategy to Secure Cyberspace"[8] in February and with the official creation of the Department of Homeland Security (DHS) on November 25, 2002. Many initiatives are already making there way through legislation as a result of strategies put forth by the new department and many of these will have a direct impact on the Information Technology community with regard to security. Some of the most profound impacts will stem directly from the previously mentioned document, "The National Strategy to Secure Cyberspace", while others will come as result of Government agency reorganizations, public and private collaboration, increased education and research, and the adoption of new technologies. The purpose of this paper is to outline these initiatives and explain how they will affect information security.

Government Takes on More Responsibility

With the formation of the Department of Homeland Security comes the biggest reorganization of government agencies in about fifty years. The new department will house 170,000 employees and 22 agencies. [6] One of the greatest challenges will be building the proposed information sharing infrastructure connecting all associated agencies across federal, state, and local levels. This infrastructure will include networks connecting the FBI's crime and terrorism databases with state and local law enforcement agencies, a secure intranet that will allow the dissemination of classified federal information to state and local entities, along with a secure video conferencing network allowing officials in Washington D.C. to communicate with all government entities within every state.[9]

With terrorism being a real and viable threat, the security of this new infrastructure and other nationally critical information infrastructures is of the utmost importance. The government has made this clear by presenting "The National Strategy to Secure Cyberspace" in February of 2003.[8] The document recognizes that cyberspace is "the control system of our country", citing the fact that many industries within the sectors of water, transportation, chemicals, energy, and manufacturing have transitioned to digital control systems (DCS) and supervisory control and data acquisition systems (SCADA). [8] These systems allow users to control vital processes and physical functions remotely over internet based connections. One can only imagine the implications of a breach in security into any of these systems.

The government admits that cyber terrorism requires complex coordination and technical expertise, which may explain why there have not been any major

disruptions in the nation's information infrastructure. However, it does realize that the threat is real and that coordinated attacks are occurring frequently. In September of 2002, an attempt was made to incapacitate the Internet by attacking the "root" servers that form the core of the Domain Name System (DNS). [7] Fortunately, the attempt failed to bring down the Internet even though it successfully debilitated several of these DNS servers. The government has outlined five priorities in the process of securing cyberspace as a result of these types of threats. The priorities include the following:

I. A National Cyberspace Security Response System
II. A National Cyberspace Security Threat and Vulnerability Reduction Program
III. A National Cyberspace Security Awareness and Training Program
IV. Securing Governments' Cyberspace
V. National Security and International Cyberspace Security Cooperation

The National Cyberspace Security Response System will be comprised of government and private institutions alike. This collaboration between government and private entities is a recurring theme throughout the strategies presented for securing cyberspace. An example of this is the Cyber Warning Information Network (CWIN). CWIN is a private IP network outside of the Internet that connects organizations such as the National Information Protection Center (NIPC), the Critical Infrastructure Assurance Office (CIAO), and several private Information Sharing and Analysis Centers (ISAC). [3] The network could be used to secretly distribute information about critical software and network vulnerabilities to affected vendors, which in turn distributes patches to critical systems before any public announcement is ever made. The security response system shall be responsible for improving national incident management; exercising cybersecurity continuity plans for federal systems; improving public-private information sharing involving cyber attacks, threats, and vulnerabilities; and establishing public-private architecture for responding to national-level cyber incidents. [8]

The National Cyberspace Security Threat and Vulnerability Reduction Program is focusing on three main channels through which to reduce vulnerabilities: 1) discourage would be attackers by creating effective programs to identify and punish cybercriminals; 2) identify and eliminate existing vulnerabilities; 3) develop new systems with less vulnerabilities and analyze emerging technologies for vulnerabilities. [8] This may seem like common sense, but these efforts have progressed at an extraordinarily slow pace pertaining to government systems. The government currently mandates certain network security policies with its agencies but fails to enforce them. In the latest assessment of information security within government entities, results showed that 14 of the 24 largest federal departments and agencies received a failing grade. [7] One step the

government is taking is to hold Chief Information Officers accountable for the security of their systems. Another initiative is the broader use of the National Information Assurance Partnership (NIAP), which is an organization consisting of the combined efforts of the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA). The NIAP tests, evaluates, and assesses software products and systems with regard to security and other consumer or producer needs.

The government realizes that part of the problem regarding information security is the lack of awareness and training at every level from home users to government system administrators. The third priority of the national strategy to secure cyberspace addresses this issue by creating a National Cyberspace Security Awareness and Training Program. More information on this topic will be discussed in the section on education and research.

The fourth priority for securing cyberspace covers securing governments' information infrastructure. As mentioned before, government systems do not have a good track record. Several initiatives will be enabled at the federal, state, and local levels and some will be geared towards additional government wide challenges. One example of these initiatives is to identify and document enterprise architectures within federal agencies. This is important not only to assesses where vulnerabilities may lie, but also to gauge how certain architectures provide advantages over others. This is a strategy that will most likely be implemented beyond the government sector into large corporations and critical industries. Hopefully information gathered from these comparisons will help educate the information security community.

The final priority presented in "The National Strategy to Secure Cyberspace" is National Security and International Cyberspace Security Cooperation. A few of the interesting goals within this priority include strengthening counterintelligence efforts in cyberspace, reserving the right to respond in an appropriate manner, and promoting North American cybersecurity by making North America a "safe cyber zone." The following is an actions and recommendations quote from "The National Strategy to Secure Cyberspace" regarding reserving the right to respond in an appropriate manner:

> *"When a nation, terrorist group, or other adversary attacks the United States through cyberspace, the U.S. response need not be limited to criminal prosecution. The United States reserves the right to respond in an appropriate manner. The United States will be prepared for such contingencies."*

This quote is somewhat vague, but it sounds as if the government is going to get very serious about the consequences for cyberterrorism. Perhaps this will

propagate through the judicial system to hold cyber attackers more accountable for there actions.

Industries See Opportunity and Government Collaboration

With the formation of the Department of Homeland Security came a steady stream of cash approved for spending on related initiatives. It's only logical that businesses jump on the opportunity to grab a piece of the homeland security pie with IT companies being no exception. More than $2 billion is expected to be spent this fiscal year on IT spending by the new department with undoubtedly a large portion going directly to information security initiatives. [6] This doesn't even include the large amounts of private industry investment into information security as the government's security policies start influencing the private sector. Microsoft has a chance to play a major role in increased information security investment while cashing in immediately from the government. The company has already formed the position of federal director of homeland security and filled it with a retired U.S. Coast Guard officer, Thomas Richey. [12] Microsoft hopes to act as a key advisor to U.S. policy makers and therefore cash in on new developments in operating systems with increased embedded security.

Despite the promising news on increased spending on information security, vendors in the field have yet to see major growth. Prior to September 11, 2001, the annual growth rate of these vendors was about 9% and it has maintained this growth rate through the end of 2002. [11] However, the Department of Homeland Security wasn't even created until November 2002, and the "National Strategy to Secure Cyberspace" wasn't officially released until February 2003. A positive note on new IT and information security spending is the contract that Unisys landed for the creation of a new information infrastructure for the U.S. Transportation Security Administration (TSA) which is now included under DHS. The contract is valued at about $221 million through the end of fiscal 2003 and is expected to continue for another two to four years. Another positive report came from the Yankee Group stating that the market for managed information security services will grow from $1.5 billion in 2002 to $2.6 by 2005. [13] With information security on the forefront of DHS policy and with the collaborative efforts between public and private sectors instantiated, information security investments are bound for double digit growth for years to come.

Collaboration between government and private industry on the issue of information security is stressed throughout the "National Strategy to Secure Cyberspace". It was also made clear that government regulation on information security policies and practices are not necessary and may actually impede information security advancement. The government argues that a single policy could create homogenous security architectures across industries, possibly making it easier to perform a coordinated attack using the same vulnerabilities. [8] Regulation may also encourage least common security practices, just marginally

passing government standards thereby inhibiting security efforts. A key part of the collaboration effort is for private sectors to form Information Sharing and Analysis Centers. These organizations will play a pivotal role in sharing information about trends in cyber attacks, vulnerabilities, and best practices. [8] As mentioned earlier, ISACs will be connected to government agencies through the newly created CWIN, which will allow information to flow securely between the ISACs and government entities.

A perfect example of private and public sector collaboration is the fact that the chemicals sector, which is comprised of trade associations and individual companies, actually participated in the unveiling of the "National Strategy to Secure Cyberspace." The corporate vice president and CIO of Dow Chemical represented the chemicals sector at the event by speaking about their specific strategies towards cybersecurity. He also stated that the "synergy between the chemical and IT industries will be even more important in the future." [14] This example may be an indication that collaborative efforts between public and private sectors will prove to play an important role in broad homeland security and specifically the advancement of securing our nations information infrastructure.

Education and Research Vamps Upwards

One of the five priorities stated by the government to secure cyberspace is to increase information security awareness and education through training, certification, and research. At the lowest level, home users and small business owners need to be aware of how their computers can be used by cyber terrorists to coordinate attacks on critical systems. They also need to be educated on how to thwart these threats by installing firewalls, virus protection software, and keeping up to date on the latest security patches. Unfortunately, large enterprise and Institutes of Higher Education (IHE) are sometimes not much better off than the general public when it comes to information security. Part of the government's strategy to increase cybersecurity is to promote private sector support for well-coordinated, widely recognized professional cybersecurity certifications. [8] The SANS Institute and CERT are two organizations that offer professional information security certifications and are recognized on the DHS website at http://www.dhs.gov/dhspublic/display?theme=26.

The government has clearly stated that increased research is vital to improving the security of our nation's information infrastructure. Recommendations are being made to stimulate research within corporations, Institutes of Higher Education, and government research institutes. The government is trying to encourage the private sector to increase research and education through collaboration efforts and possibly some tax incentives. Symantec has already taken the initiative to provide $50,000 to fund a fellowship for two Purdue students working with the University's Center for Education and Research in

Information and Assurance and Security (CERIAS). [2] CERIAS is one of the many research organizations popping up in universities across the nation. This may be a direct result of the Cyber Research and Development Act (CSRDA) just recently passed in 2002. This Act provides $900 million towards research and education to protect the nation's information infrastructure. [7] This money will go towards security related post-doctoral and senior research fellowships, research grants, the creation of computer and network security research centers under the National Science Foundation (NSF) and National Institute of Standards and Technology (NIST), college grants for undergraduate and graduate security programs, and "long-term, high risk" research. [2] The University of Texas at Dallas may be able to take advantage of CSRDA with its newly established Digital Forensics and Emergency Preparedness Institute. The institute was created on May 1, 2002 with the goal of becoming an internationally recognized "Center of Excellence in several of the major areas of research and system implementation related to digital forensics, information security and assurance, and emergency preparedness." [5] The university will eventually offer courses in information assurance, secure telecommunications networks, digital forensics, and emergency response information systems. Another IHE to take major advancements towards information security is Portland State University. Their computer science department recently announced that its curriculum in computer security meets the strict certification standards of the NSA. Core classes evaluated were cryptography, introduction to computer science, malicious code and forensics, network management and security along with a few others. [10]

Technology Gets a Push

It's only natural that technology should get a boost as a result of increased spending in IT and specifically information security. The government is already pushing new technologies within the wireless sector to improve security. According to an article by wireless news, "…the Department of Homeland Security sees wireless networking a terrorist threat." [1] Apparently government officials were even threatening to regulate the wireless networking industry if actions weren't taken to improve security immediately. Another technology likely to become mainstream in the IT industry is biometric authentication devices to replace or supplement the use of passwords and to aid in identification needs. Such devices include fingerprint readers, palm readers, retinal scanners, and facial recognition systems. The head of the science and technology office of the DHS stated just this month that such devices may start being used at U.S. borders in the future. [4]

Part of the government's strategy to secure cyberspace is to promote the development of new systems with security inherently built in. Much of the software and protocols being used on the Internet was developed before security was an issue. The use of adhoc security methods has somewhat improved information assurance, but we really won't see revolutionary security

advancements until we start building systems around security instead of security around systems. Microsoft has realized this and is most likely already developing a new operating system from the ground level with security and reliability being top priority. As mentioned earlier, the company has already hired Thomas Richey to act as a federal advisor to homeland security. New operating systems will be a very important step in the process of securing cyberspace, but we also have to look at telecommunications protocols and networking architecture. Federal agencies are now starting to document and share in-house networking architecture as a form of security assessment and also as a means to research best-practices on the subject. Technologies in networking protocols may also see a big push in the near future. IPv6, or Internet Protocol version 6, is the successor to the widely used IPv4. The new protocol has many advantages over its predecessor, but most notably is its increased address space, attribution, and native IP security (IPSEC). The government is currently assembling a task force to look into how the U.S. can effectively make the transition to the new protocol. Also under close surveillance by the government are technologies in improving Border Gateway Protocols, Domain Name Systems, address verification, and out-of-band management. The government has recognized that BGP is at the greatest risk of being targeted by attacks aimed at disrupting or degrading service on a large scale. [8] The Internet Engineering Task Force is being monitored closely by the government in its efforts to secure both BGP and DNS. Out-of-band management has been recognized as a means to thwart denial of service (DoS) attacks by sending control information to routers through a separate control network. DHS is looking into the need for increased research on this technology. The government is obviously taking a more active role in the advancement of information security technologies by promoting new developments in operating systems, network architecture, and network protocols.

Summary

Many people have questioned the ability of the new Department of Homeland Security to execute with the speed and effectiveness required to make that the United States safer in regard to terrorism. Although the department got off to a slow start, taking roughly 14 months to establish, the country can now already start to see the benefits of DHS. Initiatives to secure our nation's information infrastructure are proving to be major benefits as well as the positive economic impact it will have on the technology sector.

DHS initiatives will most largely impact information security in the areas of private and public sector collaboration, increased IT and security spending, increased education and research, and the accelerated advancement of new technologies. Collaboration between the government and private industries was stressed throughout "The National Strategy to Secure Cyberspace" while regulation was being frowned upon. The government realizes that it can not secure our

information infrastructure without combining efforts with the companies that actually own and operate the infrastructure.

Perhaps one of the most immediate impacts on information security is the amount of funds going into new secure systems, such as the one being built by Unisys to connect all components of the Transportation Security Administration. Another major effort being taken is the creation of a secure network to connect all federal agencies under DHS to local and state government entities, providing secure communications and information sharing. Spending is going to continue to grow well into the future as predicted by the Yankee Group who sees $2.6 billion dollars in the market of managed security services by 2005. [13]

Education and research in the field of information security have also felt the impact of DHS initiatives already. Universities have started taking advantage or are readying to take advantage of government dollars put aside for grants and fellowships that will go towards research institutes and undergraduate, graduate, and post-doctorate research programs based on network and information security. Even companies like Symantec are already issuing scholarships to fund students working with related university research programs. As research and education spreads, so to will awareness of the general public which will ultimately lead to more active participation in securing our nation's information infrastructure.

Emerging technologies in the area of information security will most likely see less of an immediate impact due to DHS initiatives, but it is the increased research and IT spending that will ultimately lead to new security technologies being adopted sooner than later. Increased physical system security will most likely take place first with the adoption of biometric authorization devices, followed by a transition into more secure protocols such as IPv6, and then the deployment of operating systems and network architectures specifically developed with security in mind.

The impact of DHS initiatives on information security is already making waves throughout the industry. This is apparent by rapid growth of education and research and the focus of IT companies on homeland security. The time is upon us for a revolution in the security of information and communications.

References

[1] Boutin, Paul. "Feds Label Wi-Fi a Terrorist Tool". Wired News. 6 December 2002. URL: www.wired.com/news/wireless/0,1382,56742,00.html (18 April 2003).

[2] Desmond, Paul. "Dollars, Sense and the Cyber". EarthWeb. 9 January 2003. URL: http://itmanagement.earthweb.com/columns/secugud/article.php/1567191 (18 April 2003).

[3] Fisher, Dennis. "Feds Move to Secure Net". eWeek. 10 March 2003. URL: http://www.eweek.com/article2/0,3959,922570,00.asp (18 April 2003).

[4] Gross, Grant. "Homeland Security Seeks More Tech Funds; Cyber, biometric security efforts top new agency's plans.". IDG News Service. 11 April 2003. URL: http://www.pcworld.com/news/article/0,aid,110241,00.asp (18 April 2003).

[5] Harris, Dr. E. Douglas. "A UTD Homeland Security Newsletter". The University of Texas at Dallas. February 2003. URL: http://www.utdallas.edu/research/dfepi/Newsletter_February2003.pdf (18 April 2003).

[6] Lange, Larry. "Dept. of Homeland Security: What's In It For IT?". TechWeb. 4 December 2002. URL: http://www.techweb.com/tech/security/20021204_security (18 April 2003)

[7] Sood, Ketaki. "Homeland Security Bill and Cyber Security Research and Development Act Provide Relief to Weakening Internet Security". Larta. 2 December 2002. URL: http://www.larta.org/LAVOX/ArticleLinks/021202_ketaki.asp (18 April 2003).

[8] Unknown. "The National Strategy to Secure Cyberspace". United States Government. February 2003. URL: http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf (18 April 2003).

[9] Unknown. "The National Strategy For Homeland Security: Information Sharing and Systems". United States Government. February 2003. URL: http://www.whitehouse.gov/homeland/book/sect4-2.pdf (18 April 2003).

[10] Unknown. "PSU Computer Security Curriculum Meets Strict Standards for Secure Information Systems". Portland State University. 12 March 2003. URL: http://www.marketing.pdx.edu/newsreleases/newsrelease.phtml?id=432

[11] Wagner, Mitch. "Report: Internet Weaknesses Must Be Fixed". Techweb News. 22 November 2002. URL: http://www.informationweek.com/story/IWK20021122S0005 (18 April 2003).

[12] Wagner, Mitch. "Microsoft Hires Homeland Security Director To Raise Federal Profile". InternetWeek. 15 November 2002. URL: http://www.internetweek.com/story/INW20021115S0008 (18 April 2003).

[13] Wrolstad, Jay. "Unisys Lands IT Contract for Homeland Security". Wireless Newsfactor. 19 August 2002. URL: http://www.ecommercetimes.com/perl/story/19065.html (18 April 2003).

[14] Zellen, Barry. "Chemicals Sector Helps Rollout National Strategy to Secure Cyberspace". TechnologyReports.net. 30 November 2002. URL: http://www.technologyreports.net/securefrontiers/?articleID=993 (18 April 2003).

Last Updated: July 21st, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS