Global Information Assurance Certification Paper

Protecting America's Critical Infrastructure
Kimberly Perez-Lugones
September 6, 2000

Introduction

The Internet and computer interconnectivity has revolutionized the way our government, our nation, and much of the world communicate and conduct business. The benefits have been enormous in terms of facilitating communications, business processes, and access to information. This widespread interconnectivity has posed an enormous risk to our computer systems and to the critical operations and infrastructures they support including information and communications, energy, banking and finance, transportation, water supply, emergency services, law enforcement and public health, as well as federal, state and local government services.

Since the mid-1990s, our Federal government has been struggling with the challenges of protecting America's critical infrastructures from computer-based attacks. I will cover National-level initiatives addressing information security, discuss reports from the General Accounting Office (GAO) on computer security and critical infrastructure protection, and demonstrate how each of us involved in information security whether in the private or government sector, play a role in protecting America's critical infrastructures.

Overview of National-Level Initiatives

President Clinton issued Executive Order (EO) 13010 on July 15, 1996, which established the President's Commission on Critical Infrastructure Protection (PCCIP). The PCCIP was established to investigate our nation's vulnerability to both cyber and physical threats.

The PCCIP published its report, "Critical Foundations: Protecting America's Infrastructures", in October 1997 [1]. The Commission described the potential devastating implications of poor information security from a national perspective. The PCCIP provided a listing of the many threats to the infrastructure services ranging from natural disasters, human errors, insider threats, hackers, criminal activity, industrial espionage, international terrorists, national intelligence organizations and information warfare activities.

The Commission noted the blurring of traditional boundaries and jurisdictions between the public and private sectors and stressed the need for a government-private sector partnership in the protection of our infrastructures. Recommendations from the Commission were focused into five major areas:

1. The need for a broad program of awareness and education
2. Infrastructure protection through industry cooperation and information sharing
3. Reconsideration and modernization of laws related to infrastructure protection
4. A revised program of research and development
5. A national structure

As a result of the findings and recommendations of the PCCIP, President Clinton issued two new directives designed to strengthen the Nation's defenses against terrorism and unconventional threats: Presidential Decision Directives (PDD) 62 and 63. Both were approved on May 22, 1998; the PDD-62 addresses the national problems of countering terrorism in all its varied forms while the PDD-63 focuses specifically on protecting the Nation's critical infrastructures from both physical and "cyber" attack.

The PDD-63 formally created the structure for the government-private sector partnership recommended from the PCCIP. A position for a new National Coordinator (for Security, Infrastructure Protection and Counter-Terrorism) within the Executive Office of the President was created for coordinating the government and private partnership.

The PDD-63 set up the Critical Infrastructure Assurance Office (CIAO) under the Department of Commerce and the National Infrastructure Protection Center (NIPC) under the sponsorship and guidance of the Federal Bureau of Investigation (FBI). The PDD-63 established the framework for voluntary Information Sharing and Analysis Centers (ISACs), to help coordinate information sharing.

The quick summary of national initiatives from 1996-1998 illustrate that leaders in the highest offices of our government recognize that computer-based risks to our nation's critical infrastructures require coordination and cooperation across federal agencies, public and private sectors entities and even other nations. This is a complex and challenging problem facing our nation. The challenge is having groups and entities with different goals/objectives, work ethics and business practices (whom have traditionally not "trusted" each other) labor together

and rely on each other to ensure their infrastructures are protected. Another challenge to protecting the critical infrastructure is the lack of sound information security programs at virtually every major agency. How can the federal government lead the nation in protecting America's critical infrastructure when they can't fix the problems within their own agencies?

GAO's Findings on Computer Security and Critical Infrastructure Protection

In a testimony before the Subcommittee on Technology, Terrorism and Government Information, Committee on the Judiciary, U.S. Senate on October 6, 1999, the GAO discussed the computer security aspects of critical infrastructure protection and focused on federal agency performance [2].

The GAO noted long-standing computer security weaknesses that place federal operations at serious risk. The GAO cited 22 of the largest federal agencies as having significant computer security weaknesses including controls over access to sensitive systems and data, software developments/changes, and contingency plans. Poor security program management was identified as the leading cause of weak information security. On a positive note, the GAO found that organizations with superior security programs managed their risks through a cycle of risk management activities.

The GAO also addressed the need for defining key federal agency roles and responsibilities. This also included the evaluation of an agency's performance, congressional oversight, and additional levels of technical and funding support in ensure that critical infrastructure objective are met.

National Plan for Information Systems Protection

The *National Plan for Information Systems Protection: Version 1.0: An Invitation to a Dialogue* was released January 7, 2000 by the White House as the first major element in a more comprehensive effort to protect the nation's information systems and critical assets [3].

The PDD-63 directed the development of the National Plan. Version 1.0 of the National Plan primarily focuses on the federal efforts. Subsequent versions will include specific roles that industry, state and local governments will play in protecting privately owned infrastructures.

The goal of the National Plan is to achieve a critical information systems defense. An initial operating capability is scheduled by December 2000 and fully operating by May 2003. The Plan (1) identified the risks arising from the nation's dependence on computer networks for critical services, (2) recognized the need for the federal government to take the lead in addressing critical infrastructure risks and to serve as a model for information security, and (3) outlined key concepts and general initiatives to help achieve these goals.

The Plan was designed around three broad objectives:

1. Prepare and Prevent: Those steps necessary to minimize the possibility of a significant and successful attack on our critical information networks. Building an infrastructure that remains effective in the face of such attacks.
2. Detect and Respond: Those actions required identifying and assessing an attack in a timely way, contain the attack, quickly recover from it, and reconstitute affected systems.
3. Build Strong Foundations: The things we must do as a Nation to create and educate the people and the organizations of both government and private sector. This will allow us to "prepare and prevent" or if needed, "detect and respond" to any attack on our critical information networks.

In a statement issued by the GAO [4], they generally supported the National Plan for Information Systems Protection as an important and positive step toward building a cyber defense but felt the Plan relied too heavily on legislation and requirements that are outdated. The GAO also commented on improvements that could be made to the Plan to better develop a public-private partnership.

"ILOVEYOU" Virus Highlights Need for Improved Alert and Coordination Capabilities

The ILOVEYOU virus demonstrated the challenges of being able to "detect and respond". While the federal government was implementing mechanisms that would help agencies to fight off such an attack, it was not effective at detecting this virus and warning agencies about the imminent threat. Agencies such as NIPC and FedCIRC had limited impact on being able to mitigate this attack.

In another GAO testimony [5] they discussed the virus and the impact it had on federal agencies. The GAO report stated, "The potential for more catastrophic damage is significant". Further, the GAO noted that over 100 countries

have or are developing computer attack capabilities. These concerns highlight the need for improved alert and coordination capabilities to protect our nation's critical information systems from all possible attacks.

Cyber Security Information Act - H.R. 4246

H.R. 4246 [6] was introduced to the 106th Congress on April 12, 2000 with the aim of addressing the private sector's concerns about voluntarily sharing information with the government. Some of the concerns raised by the private sector are possibilities that they could face antitrust violations for sharing information with other industry partners, have their information be subject to the Freedom of Information Act (FOIA), or face potential liability concerns for information shared in good faith.

In response to these concerns, H.R. 4246 has been written to:

- Protect information being provided by the private sector from disclosure by federal entities under FOIA or disclosure to or by any third party,
- Prohibit the use of the information by any federal and state organization or any third party in any civil actions, and
- Enable the President to establish and terminate working groups composed of federal employees for the purposes of engaging outside organization in discussion to address and share information about cyber security.

In the latest major action for the bill, the Subcommittee on Government Management, Information and Technology, Committee on Government Reform in the House of Representative held hearings on June 22, 2000. In a prepared statement [7] the GAO noted that H.R. 4246 can help build the meaningful private-public partnerships but that the federal government must be a model of good information security. The GAO also noted that the federal government might not yet have the right tools in identifying, analyzing, coordinating, and disseminating the type of information the bill envisions collecting from the private sector.

David Sobel from the Electronic Privacy Information Center (EPIC), expressed concerns over the bill's Freedom of Information Act (FOIA) exemptions [8]. Mr. Sobel expressed concerns that the proposed critical infrastructure exemption would hide from the public possible information about government activities. These activities could be partnerships with the private sector or an adverse impact on the public's right to know about unsafe practices being conducted by the private sector.

Challenges to Building a Comprehensive Strategy for Information Sharing and Coordination

On July 26, 2000 the GAO reported on the challenges of building a comprehensive strategy for information sharing and coordination [9]. While this latest GAO report did not address any "new" ideas or concepts in the critical infrastructure protection, I found it to be one of the more interesting testimonials. It summarized the efforts, challenges, and importance in protecting our infrastructure with existing recommendations and methodologies identified in previous GAO reports. This same report summarized and recognized a number of government and private sector organizations that facilitate public-private sector information sharing. Even the SANS Institute received a mention from the GAO.

Summary

The federal government to ensure the protection of the nation's critical infrastructure has initiated a number of positive actions. They understand the need for a strong public-private sector partnership in achieving these goals. Steps are being taken to strengthen the security at our federal agencies, bills are being introduced to foster information sharing, and processes are being established for gathering information on threats and protection.

Nevertheless, many challenges exist and must be overcome. Trust needs to be established between stakeholders and information sharing. Coordination issues need to be resolved and public - private sector responsibilities need to be clarified. There also remains a need for technical expertise to be developed in both sectors.

I also believe that a "buy-in" from management on the importance of information security is the key element for any organization's critical infrastructure protection. Until the leaders of our government and private industries understand and value the importance of strong information protection and recognize that computer security operations are vital to their mission, we may never truly have computer security on our network infrastructures.

References

1. The Report of the President's Commission on Critical Infrastructure Protection, "Critical Foundations: Protecting America's Infrastructures", October 1997. URL: http://www.pccip.gov/
2. Testimony of Jack L. Brock, Jr., Director, Governmentwide and Defense Information Systems Accounting and Information Management Division U.S. General Accounting Office, before the Subcommittee on Technology, Terrorism and Government Information, Committee on the Judiciary, U.S. Senate. "Critical Infrastructure Protection: Fundamental Improvements Needed to Assure Security of Federal Operations." GAO/T-AIMD-00-7. October 6, 1999. URL: http://www.gao.gov/
3. Release by the White House. "Defending America's Cyberspace: National Plan for Information Systems Protection." January 7, 2000. URL: http://cryptome.org/cybersec-plan.htm
4. Testimony of Jack L. Brock, Jr., Director, Governmentwide and Defense Information Systems Accounting and Information Management Division U.S. General Accounting Office, before the Subcommittee on Technology, Terrorism and Government Information, Committee on the Judiciary, U.S. Senate. "Critical Infrastructure Protection: Comments on the National Plan for Information Systems Protection." GAO/T-AIMD-00-72. February 1, 2000. URL: http://www.gao.gov/
5. Testimony of Jack L. Brock, Jr., Director, Governmentwide and Defense Information Systems Accounting and Information Management Division U.S. General Accounting Office, before the Subcommittee on Financial Institutions, Committee on Banking, Housing and Urban Affairs, U.S. Senate. "Critical Infrastructure Protection: "ILOVEYOU" Computer Virus Highlights Need for Improved Alert and Coordination Capabilities." GOA/T-AIMD-00-181. May 18,2000. URL: http://www.gao.gov/
6. H.R. 4246, "Cyber Security Information Act", April 12, 2000. Sponsor: Rep Thomas Davis of Virginia. URL: http://thomas.loc.gov/cgi-bin/query
7. Testimony of Joel C. Willemssen, Director, Civil Agencies Information Systems Accounting and Information Management Division U.S. General Accounting Office, before the Subcommittee on Government Management, Information and Technology, Committee on Government Reform, House of Representatives. "Critical Infrastructure Protection: Comments on the Proposed Cyber Security Information Acton of 2000." GOA/T-AIMD-00-229. June 22, 2000. URL: http://www.gao.gov/
8. Testimony of David L. Sobel, General Counsel, Electronic Privacy Information Center, before a hearing of the Subcommittee on Government Management, Information, and Technology. "Hearing on H.R. 4246, the Cyber Security Information Act." June 22, 2000. URL: http://www.epic.org/security/cip/hr4246_testimony.html
9. Testimony of Jack L. Brock, Jr., Director, Governmentwide and Defense Information Systems Accounting and Information Management Division U.S. General Accounting Office, before the Subcommittee on Government Management, Information and Technology, Committee on Government Reform, House of Representatives. "Critical Infrastructure Protection: Challenges to Building a Comprehensive Strategy for Information Sharing and Coordination." GAO/T-AIMD-00-268. July 26, 2000. URL: http://www.gao.gov/