Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Securing Our Critical Infrastructures

As technology advances, so do the vulnerabilities and security threats to our critical infrastructures. We must constantly re-evaluate the critical infrastructure sectors to better prepare ourselves for whatever challenge is thrown at us, be it natural or man-made. Strong consideration of the infrastructure interdependencies and the effects of loosing one or more in an attack is essential to prepare a contingency plan that will allow for the preservation of our critical assets. In the event of a successful attack, limi...

Copyright SANS Institute
Author Retains Full Rights

AD

Securing Our Critical Infrastructures

Mr. Chris A. Brooks
Certified Novel Administrator (CNA), Certified Network Analyst I (CNA-I)
GSEC Practical Version 1.4b, Option 1
October 11, 2002

I. Introduction

In the wake of the September 11, 2001 attack on United States, infrastructure security has become the top priority of our government and many commercial organizations. All aspects of our society today are heavily interdependent upon a vast array of Information Technology (IT). This technology is a core component of our national defense, economic prosperity and touches our every day life. The most critical infrastructures include banking and finance, telecommunications, energy (gas and electric), transportation, emergency services, and essential government services.

Today, computer networks connect and control everything from trains to airplanes to the stock exchange. US National Security Advisor, Condoleeza Rice stated in a speech in March 2001, "Today, the cyber economy is the economy…. Corrupt those networks and you disrupt this nation."[1] No truer words were spoken when we look at the most recent event of the attacks on the World Trade Center and the Pentagon. Transportation, telecommunications, emergency services, and financial institutions were hit the hardest when the critical infrastructure collapsed with the Twin Towers.

II. Critical Infrastructures

The incapacitation or destruction of our critical infrastructures would have a crippling impact on the defense and economic security. Our vital infrastructures are so interconnected that the failure of one greatly affects the others. Let's take a brief look at each critical infrastructure component.

- Transportation - allows for the organized flow of goods and people within and outside our borders. This organized flow makes it possible for the United States to be the leader in the global economy.

- Oil and Gas Production and Storage – fuels the transportation services, as well as manufacturing operations and home utilities.

[1]Saxton, Jim. "Security in the Information Age: New Challenges, New Strategies." May 2002, URL: http://www.house.gov/jec/security.pdf .

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

- Water Supply – provides a continuous flow of water for agriculture, industry, business, firefighting, and to our homes.

- Emergency Services – in local communities across the country responds to fire, police, and medical needs by preserving property and saving lives on a daily basis.

- Government Agencies – consists of local, state, and federal agencies that provide essential services to the public.

- Banking and Finance – manages trillions of dollars from the deposit of our individual paychecks to the transfer of huge amounts of money supporting global enterprises.

- Electricity – consists of the generation, transmission, and distribution systems that are essential to all other infrastructures and to every aspect of the economy.

- Telecommunications - revolutionized by the huge advances in IT over the last 20 years and has become an information and communications infrastructure that includes Public Telecommunications Network (PTN), the internet, and the huge number of computer systems installed for home, business, and government use.

III. IT Revolution

On June 21, 2001, Lawrence K. Gershwin of the National Intelligence Council told the Joint Economic Committee that the "information technology revolution represents the most significant global transformation since the Industrial Revolution beginning in the mid 18th-century . . . no country in the world rivals the United States in its reliance, dependence, and dominance of information systems. The great advantage we derive also presents us with unique vulnerabilities."[2]

Any technology that has improved our infrastructure can also be used to disable it. Close to half of all computer capacity and 60% of Internet assets are in the United States, causing us to be one of the most technologically advanced and, at the same time, the most dependent user of information technology. Our dependence on the IT infrastructure has created cyber vulnerabilities that we are still trying to understand. In addition to the disruption of information and communications, we also face the possibility that someone will mount an attack

[2] Bennett, Robert F. "Security in the Information Age: New Challenges, New Strategies." May 2002, pg.2. URL: http://www.house.gov/jec/security.pdf .
.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

against other infrastructures by exploiting their dependence on computers and telecommunications (Figure 1).

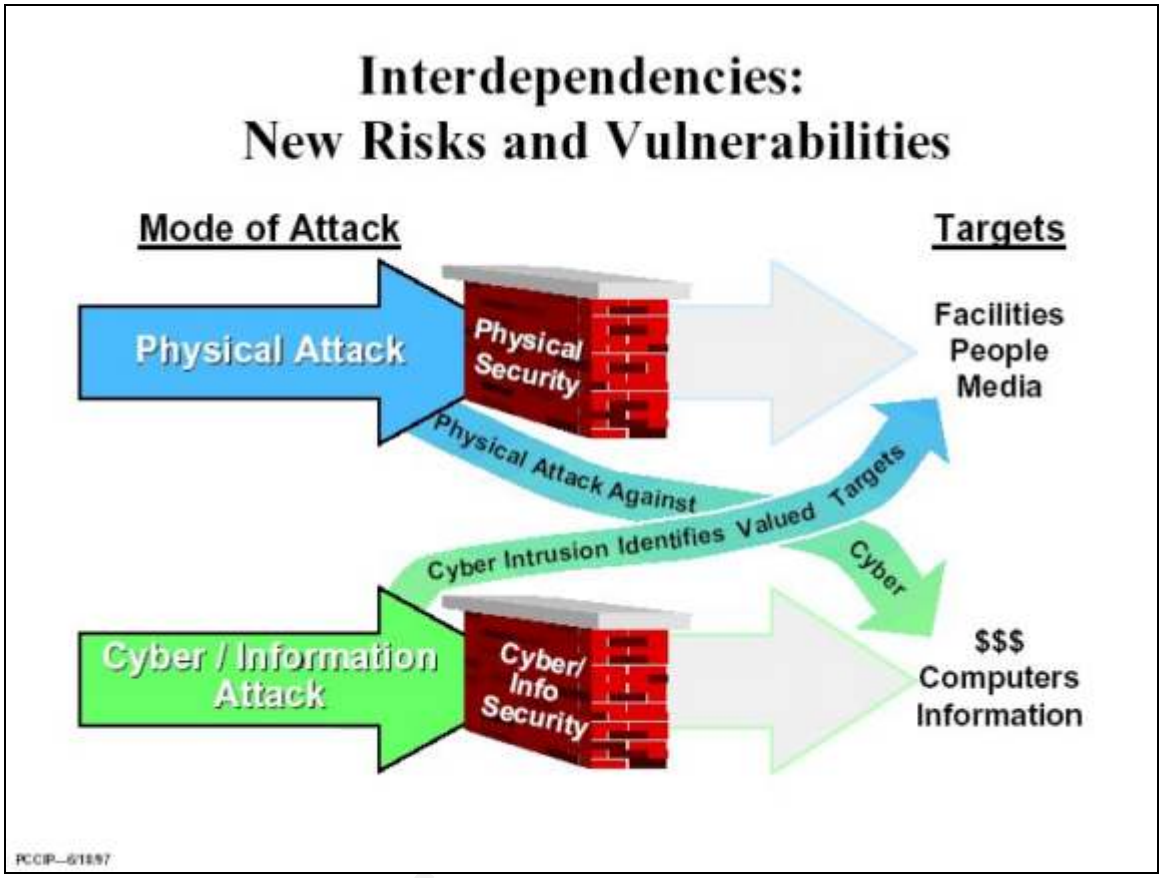

Figure 1. Taken from the President's Commission on Critical Infrastructure Protection Overview Briefing, June 1997. URL: http://www.ciao.gov/resource/pccip/brief697.pdf

IV. Critical Infrastructure Protection

In order to protect the infrastructures, we must first know how they interconnect and what the effects on the other infrastructures might be if one or more are disabled. Presidential Decision Directive (PDD) 63 on Critical Infrastructure Protection (CIP) describes critical infrastructures as the physical and cyber-based information systems essential to the minimum operations of the economy and the government.

An initial vulnerability assessment was conducted on each sector of the economy and government to determine what might be targeted for an attack. Minimum essential infrastructure (MEI) were determined and included in the sector assessments. The following chart depicts the status of the assessments in each sector:

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Infrastructure Sector	Vulnerability Assessment	Remedial Plan
Banking and Finance	Some Assessments	No Remedial Plan
Electric Power, Oil, and Gas	Some Assessments	No Remedial Plan
Emergency Fire Services	No Assessments	No Remedial Plan
Emergency Law Enforcement	No Assessments	No Remedial Plan
Information and Communication	No Assessments	No Remedial Plan
Public Health Services	No Assessments	No Remedial Plan
Transportation	No Assessments	No Remedial Plan
Water Supply	Some Assessments	No Remedial Plan

Table 1. From the Security in the Information Age: New Challenges, New Strategies: Joint Economic Committee, United States Congress, May 2002.

V. Information Sharing and Analysis

The government and industry cannot afford to protect everything to the same degree and as a result, the security planners must prioritize what core missions and supporting services are the most critical. Both the government and industry must cooperate to assess the infrastructures, discover the vulnerabilities, and provide remedies for those vulnerabilities.

Potential attacks posed on our infrastructures do not fall within our existing institutional arrangements and assignments of responsibility. Our government is not structured to take quick and decisive actions to incidents that cross many departments and agencies that interact with specific segments of the economy and their supporting infrastructures.

Sharing of information prior to a crisis is very important. Under the Clinton administration, the President's Commission on Critical Infrastructure Protection (PCCIP) was created by the Attorney General in response to PDD 39 in regard to terrorist threats to the United States. The PCCIP identified information sharing as one of the most pressing needs in protecting critical infrastructure. The report stated,

> The government and private sector share substantially the same national information infrastructure. Both have been victims of unauthorized computer intrusions, theft, and disruption. In our view, the line separating threats that apply only to the private sector from those associated with traditional national security concerns must give way to a concept of shared threats. Shared threats demand a shared response, built from increased partnerships between government and the owners and operators of our infrastructures.[3]

[3] "Critical Foundations: Protecting America's Infrastructures, The Report of the President's Commission on Critical Infrastructure Protection." October 1997, Chapter 3, p19. URL: http://www.ciao.gov/resource/pccip/PCCIP_Report.pdf

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

It makes sense for both the government and the private sector to share information since they are both targeted for attack.

Even though the private sector is on the front line of being targeted for attack, it has no access to government information concerning possible attacks due to most of it being classified. In addition, the federal government, with its unique information and analytical capabilities, lacks specific information concerning computer attacks outside the government sector but still contained within the U.S.

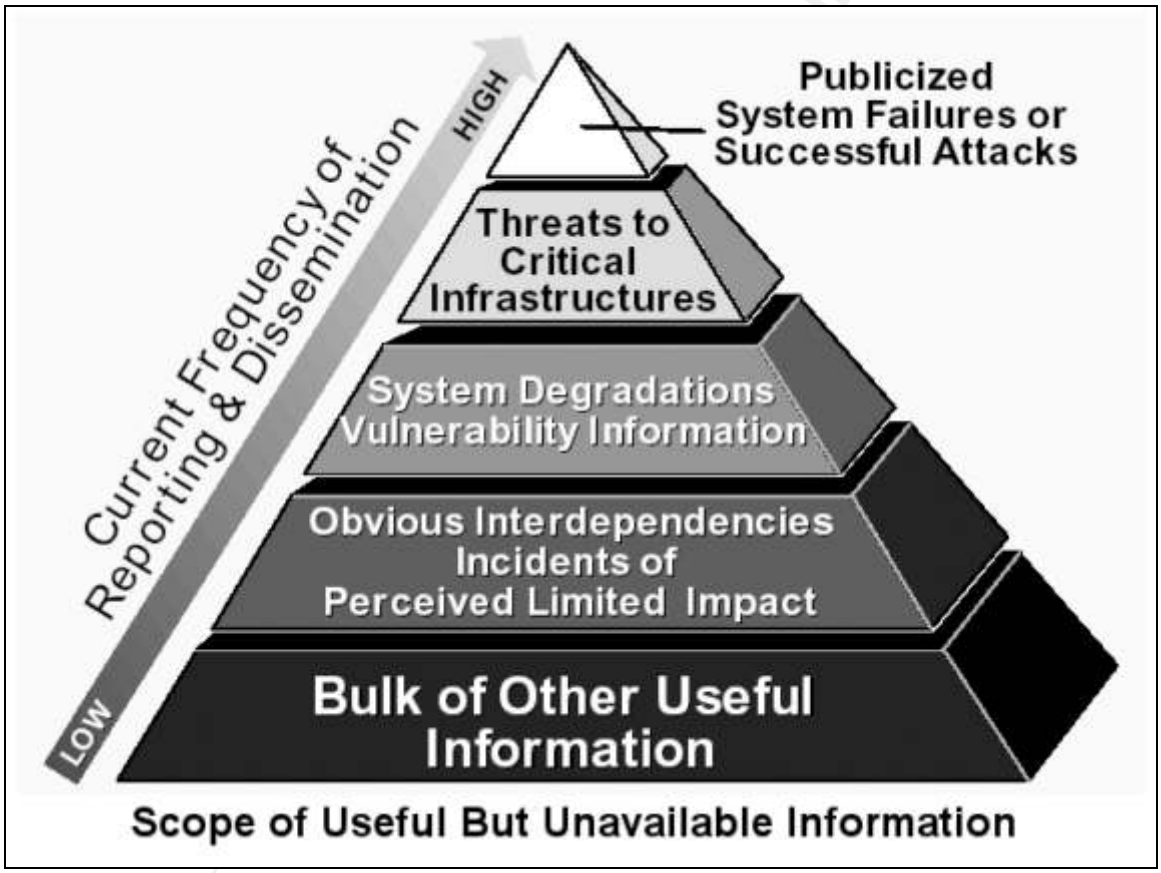

Figure 2. Taken from the The President's Commission on Critical Infrastructure Protection Final Report. URL: http://www.ciao.gov/resource/pccip/PCCIP_Report.pdf

PDD 63 encouraged the creation of Information Sharing and Analysis Centers (ISACs) in the private sector. ISACs play a key role by encouraging the member organizations to exchange information relating to threats, vulnerabilities, attack solutions, countermeasures, and best practices.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

ISACs have the following limitations:

1. Not all critical industries are members
2. Are evolving industry by industry
3. Being developed to meet the specific needs of each sector
4. Sole dependence on an industry-specific focus fails to give government or industry crosscutting information

Little use can be made of information that has not been analyzed. The need for comprehensive analysis is critical to support the decision-making process in how to respond to attacks. Learning to properly identify potential attack patterns or distinguish the intent of what appears to be widespread or random computer viruses will require a new discipline. The terrorists of tomorrow will employ a wider arsenal of destructive tools for which will require stronger analytical skills to combat and repel the attacks.

Along with the efforts to improve our capabilities to analyze the information, there is a need to incorporate a warning process for critical infrastructures. The importance of both sending and receiving the information, as well as a way to determine if the information has been sent and actions taken need to be included in the warning process. Our current measuring stick for determining this is the media. The news, be it in print or broadcast via radio and television, let's us know if people have or are taking action in response to a specific threat. Follow-up stories often let us know if the threat information was all hype and the strong warning was overkill or if the warning was not strong enough, causing the threat to linger a while longer.

VI. Security and Cyber Space

Securing our internet infrastructure is an important element in securing our critical infrastructures. Our critical infrastructures, such as transportation, oil and gas production, water, emergency services, and banking and finance, are all interconnected by the internet. Systematic cyber attacks forcing any one of the critical infrastructures to shutdown can affect any or all of the others.

A good example of a less physical but economically significant attack was orchestrated a week after the attacks on September 11, 2001. The attack was called NIMDA ("ADMIN" spelled backwards), and it was a sharp wake-up call to a nation so heavily dependent upon computer networks. NIMDA was an automated cyber attack. It was a blend of a virus and a worm, and it propagated across the nation with lightning speed. It went from nonexistent to nationwide in an hour and lasted for days, attacking more than 100,000 computer systems by the end of the first day. NIMDA caused significant problems in well-protected industries, forcing many firms offline, shutting down customer access, and requiring some companies to rebuild their systems entirely. The estimated cost

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

of the overall financial impact of the NIMDA virus may have been as high as $13 billion in 2001.

Two months prior to the NIMDA attack another cyber attack called Code Red infected over 150,000 computer systems in 14 hours and caused billions of dollars in losses. Figures 3 and 4 below were extracted from an animated gif file which was created using data on the spread of the Code Red virus within a 24-hour period. At the start of the data collection there were 159 victims reportedly affected by Code Red as shown in Figure 3. By the end of the 24-hour period, there were 341,015 victims as shown in Figure 4. It took weeks to clean and repair the damage created by this virus.

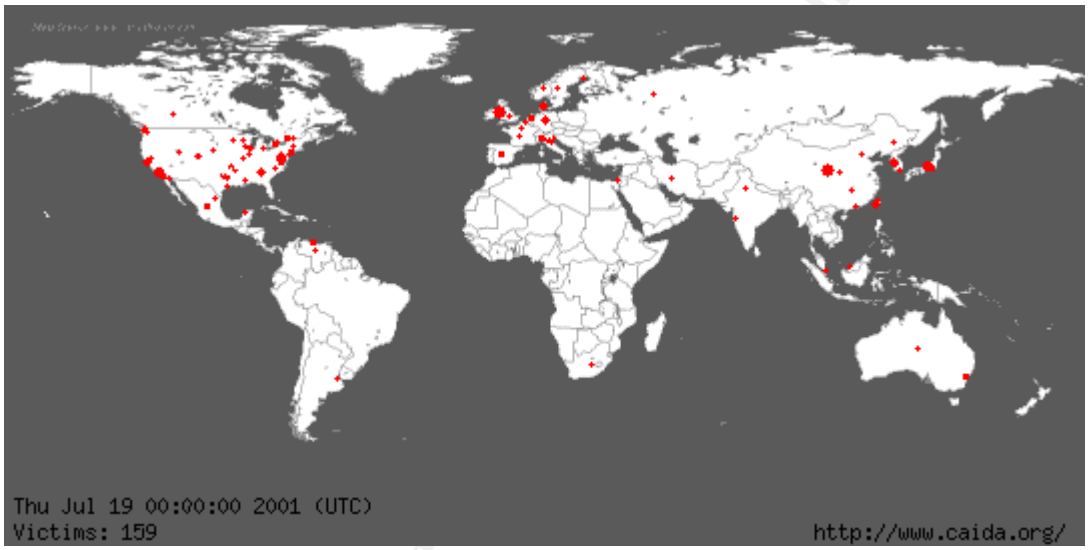

Figure 3. This is frame 1 of an animated file of the Code Red virus. It illustrates how fast and wide spread a virus can travel.

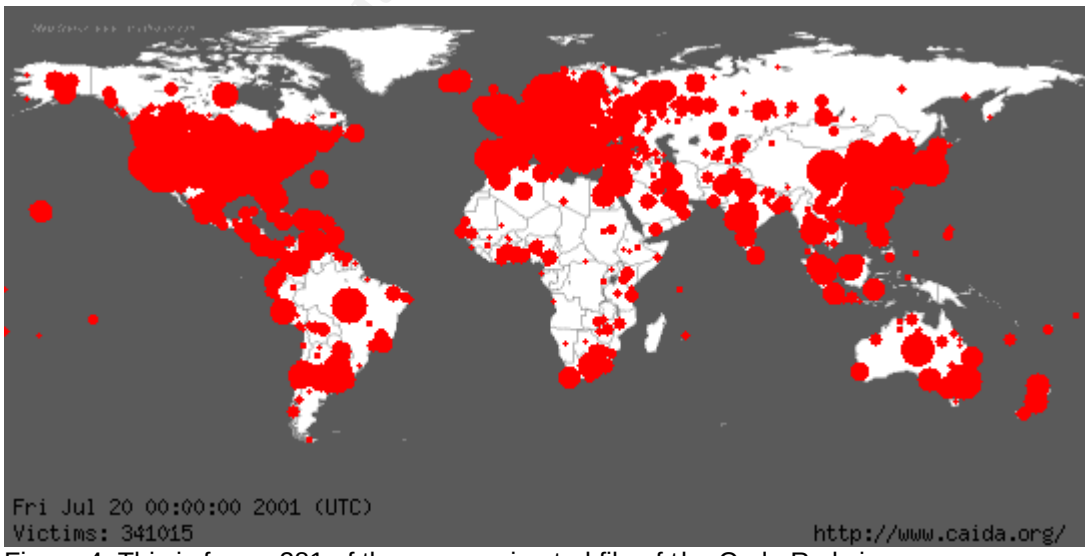

Figure 4. This is frame 281 of the same animated file of the Code Red virus. (http://www.jump.org.uk/caida_code_red_animations/newframes-small-log.gif)

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

The sophistication and destructiveness of cyber attacks are ever increasing, as is the volume of attacks. Carnegie Mellon University's Computer Emergency Response Team's (CERT) Coordination Center (http://www.cert.org/) reported over 3,700 attacks in 1998 and have reported over 143,505 attacks by the end if Q2 of 2002[4].

Identifying and providing a remedy for computer system and network vulnerabilities is paramount in keeping our internet infrastructure secure. The process of securing systems and networks must be continuous process because new vulnerabilities are created and discovered regularly.

Prior to placing a system or device on a network, all precautions must be taken to secure it. This entails applying service patches to the Operating System (OS), closing all unnecessary ports, installing an antivirus package (if the OS can support one), and restricting access to the system or device

Service patches for a specific operating system can be found at the following:

Apple

http://www.info.apple.com/usen/security/index.html http://www.cert.org/

Linux

http://www.linux-sec.net/
http://www.nsa.gov/selinux/
http://www.sonic.net/hypermail/security/
http://www.redhat.com/solutions/security/
http://www.linuxsecurity.com/
http://www.cert.org/

Unix

http://www.freebsd.org/security/index.html
http://www.sun.com/bigadmin/
http://www.cert.org/
http://online.securityfocus.com/

Windows

http://www.microsoft.com/security/
http://online.securityfocus.com/
http://www.cert.org/

Antivirus

Installing an antivirus application and keeping up with the latest virus signatures is a good start in protecting computer systems. Symantec and McAfee are just two of the leading provides of home and corporate antivirus protection.

[4] http://www.cert.org/stats/cert_stats.html

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Security News Letters and Bulletins

Subscribing to computer security electronic letters, bulletins and visiting online security websites regularly will assist IT departments in keeping up-to-date on the latest security issues, news and views. The following is but a partial list.

Vendor Mailing Lists

- Red Hat
- SuSE
- Slackware
- Debian
- Immunix
- Linux-Mandrake
- Turbolinux
- Microsoft

Security Mailing Lists

- SecurityFocus lists
  Bugtraq, Incidents, Vuln-dev, Focus-Linux, SF-News and many more.
- LinuxSecurity.com
  Excellent weekly updates on Linux security.
- Firewalls
  Original Firewalls mailing list, unmoderated
- Firewall-Wizards
  Firewall mailing list, moderated by firewall guru Marcus Ranum.
- Sans
  Sans weekly and monthly newsletters
- Cert
  Cert Advisories
- SAFER
  Security Alert for Enterprise Resources

Security and Hacking Websites

- LinuxSecurity.com
  Linux security news and resources.
- SANS
  System Administration, Networking and Security Organization
- CERT
  Computer Emergency Response Team
- CIAC
  Computer Incident Advisory Capability

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

- Security Focus
  Extensive vulnerability database, Custom security articles, and Security Focus mailing lists
- Security Portal
  Portal to many security sites and articles.
-
- Neohapsis Archives
  Achives of many security and vendor lists
- Insecure.org
  Nmap, list archives, exploits, and other excellent reading
- Packet Factory
  Network and security tools galore
- Attrition.org
  News, crypto, downloads, and the hacked web page mirror.
- hack.co.za
  Exploit archives
- Rootshell
  Exploit archives
- Anticode
  Exploits
- Phrack Magazine
  Phrack Magazine and archives, a must read.
- 2600 The Hacker Quarterly
- L0pht Heavy Industries
  Now part of @stake.
- Technotronic
  News, security archives, exploits, and more.
- Packetstorm
  Searchable and downloadable database of hacking tools, countermeasures and documents

VII. Conclusion

As technology advances, so do the vulnerabilities and security threats to our critical infrastructures. We must constantly re-evaluate the critical infrastructure sectors to better prepare ourselves for whatever challenge is thrown at us, be it natural or man-made. Strong consideration of the infrastructure interdependencies and the effects of loosing one or more in an attack is essential to prepare a contingency plan that will allow for the preservation of our critical assets. In the event of a successful attack, limiting the amount of damage and quickly redistributing the assets to maintain a minimum essential infrastructure is critical in keeping the defense and national economy functioning. Continuity is the key to success.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

A strategy must be developed that will include the sharing of information between the government and the private sector if we are to keep our critical infrastructure secure. Each has their strengths and weaknesses, and by collaborating with one another, we can obtain the best of both worlds in creating a world-class defense against the physical and cyber attacks that threaten the United States.

A common means of communicating the overall critical infrastructure policy is essential. A joint strategy developed between the government and the private sector would lay out the respective rolls and responsibilities that each will have. This would also help establish a common base with Congress and the American public.

Keeping our critical infrastructures protected and healthy is important to the survival of our defense and economy.

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

References

[GAO-01-323] Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities. April 2001
URL: http://www.gao.gov/new.items/d01323.pdf

Security in the Information Age
URL: http://www.house.gov/jec/security.pdf

2002 Computer Crime and Security Survey
URL: http://www.gocsi.com/pdfs/fbi/FBI2002.pdf

Secure Infrastructure Design
URL: http://www.cert.org/archive/pdf/Secure_Infrastructure_Design.pdf

Common Defense Against Uncommon Threats: The Federal Role in Critical Infrastructure Protection
URL: http://www.ciao.gov/resource/pccip/CommonDefense.pdf

Critical Foundations, Protecting America's Infrastructures, Introduction
URL: http://www.ciao.gov/resource/pccip/intro.pdf

Critical Foundations, Protecting America's Infrastructures, 1997 Briefing
URL: http://www.ciao.gov/resource/pccip/cfbrief.pdf

Critical Infrastructure Protection Strategic Simulation Report
URL: http://www.ciao.gov/resource/pccip/StrategicSimulation.pdf

Economic Impacts of Infrastructure Failures
URL: http://www.ciao.gov/resource/pccip/EconomicImpacts.pdf

Cyber Protests: The Threat to the U.S. Information Infrastructure
URL: http://www.nipc.gov/publications/nipcpub/cyberprotests.pdf

National Strategies and Structures for Infrastructure Protection
URL: http://www.ciao.gov/resource/pccip/NationalStrategiesStructures.pdf

Presidential Decision Directive (PDD) 63
UTL: http://www.ciao.gov/resource/paper598.pdf

Executive Order 13231 - Critical Infrastructure Protection in the Information Age (October 16, 2001)
URL: http://www.ciao.gov/resource/eo13231.html

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Executive Order 13228 - Establishing the Office of Homeland Security and the Homeland Security Council (October 8, 2001)
URL: http://www.ciao.gov/resource/eo13228.html

The President's Commission on Critical Infrastructure Protection Final Report
URL: http://www.ciao.gov/resource/pccip/PCCIP_Report.pdf

The President's Commission on Critical Infrastructure Protection, An Overview Briefing -- June 1997
URL: http://www.ciao.gov/resource/pccip/brief697.pdf

Information Technology—Essential But Vulnerable: How Prepared Are We for Attacks?
URL: http://www.cert.org/congressional_testimony/Pethia_testimony_Sep26.html

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 24th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced