# NATIONAL INFRASTRUCTURE ADVISORY COUNCIL

## PRIORITIZING CYBER VULNERABILITIES

# FINAL REPORT AND RECOMMENDATIONS BY THE COUNCIL

**October 12, 2004**

**MARTIN G. MCGUINN**
**WORKING GROUP CHAIR**
**CHAIRMAN AND CHIEF EXECUTIVE OFFICER**
**MELLON FINANCIAL CORPORATION**

# Table of Contents

**ACKNOWLEDGEMENTS**

## Contributors:

**Working Group Members:**

Martin G. McGuinn – Mellon Financial Corporation
John Chambers – Cisco Systems
Marilyn Ware – American Water

**Study Group Members:**

Susan Vismor – Mellon Financial Corporation
Bruce Larsen – American Water
Christopher Terzich – Wells Fargo & Company
Kenneth Watson – Cisco Systems
Dan Bart – Telecom Industry Association
Lou Leffler – North American Electric Reliability Council
Teresa Lindsey - BITS
David Thompson - Telecom Industry Association
Tim Zoph – Northwestern Memorial Hospital

**Department of Homeland Security Support:**

Leslie Burchett – Infrastructure Coordination Division
Gail Kaufman - Infrastructure Coordination Division
Brett Lambo - Infrastructure Coordination Division
Tran Trang - National Cyber Security Division
Nancy Wong - Infrastructure Coordination Division

**Additional Resources:**

Scott Borg – Institute for Security Technology Studies, Dartmouth College

## INTRODUCTION

During a meeting with the President in July 2003, two questions were asked of the Council. First, the President asked whether the Internet could be hardened against attack. Second, he asked whether we were prioritizing our actions against cyber attack. These two questions prompted the Council to create working groups to study each problem and develop reports and recommendations. This is the report of the NIAC's Working Group to prioritize cyber vulnerabilities.

The President's question was timely, since "cyber attacks, or breaches of information security, appear to be continuing, and few are willing to ignore the possibility that the severity of future attacks could be much greater than what has been observed to date."[1] The latest *Symantec Internet Security Threat Report*[2] revealed that in a typical week, 48 new software vulnerabilities around the world are uncovered. On average, hackers are now able to exploit vulnerabilities within days of their announcement. The trend is for even shorter times between vulnerability discovery and first exploitation. Security practitioners predict "zero-day attacks" in the near future, when criminals will release malicious code within minutes of the disclosure of vulnerability. These attacks, along with viruses and worms, can cause varying degrees of harm, from the manageable to the serious. For many organizations, the cost to prepare for, react to, and recover from these attacks has become an added cost.

The reach and economic impact of these attacks cannot be underestimated. Reports by various consulting firms, security companies, and research institutions vary worldwide, from a few million dollars per year to billions of dollars per year. "The reliability of these estimates is often challenged; the underlying methodology is basically anecdotal…. Estimates of the macroeconomic costs of cyber attacks are speculative. As long as any cyber attack is limited in scope and short-lived, it is likely that macroeconomic consequences will be small. But the ability to recover quickly is important, since the length of time computers are affected is an important determinant of the costs. It may be almost as important for firms to address their abilities to restore operations as to insulate themselves from potential attacks."[3] A pilot survey conducted by the Department of Justice in 2001 found that 74 percent of businesses have been a victim of cyber crime. Even though the precise financial impact of cyber attack cannot be measured, consequences dictate this is a serious issue warranting action by critical infrastructure businesses and governments.

A large and growing number of industries rely on network-based systems for key business functions. Some major companies report that transactions involving 90 percent of their revenue are processed over networked systems. Just as there is no standard methodology for accurately determining the financial impact of cyber attacks and incidents, dependencies on networked systems and among critical infrastructure sectors are not well known. In 2003, the Sobig virus

[1] Brian Cashell, William D. Jackson, Mark Jickling, and Baird Webel, "The Economic Impact of Cyber-Attack," CRS Report for Congress, April 1, 2004, summary page.

[2] Symantec Internet Security Threat Report, Volume VI, September 2004, available at http://enterprisesecurity.symantec.com

[3] Ibid.

temporarily shut down 23,000 miles of one railway system, but not other railways, due to an unforeseen dependency. In August 2003, the Slammer worm caused a major bank's automated teller machines to go off-line for several hours, but not the ATMs of other banks.[4]

It is in this context of widespread dependency on technologies under constant, escalating attack that the Council was tasked with investigating the relative vulnerability of various sectors of the U.S. critical infrastructure to cyber attack.

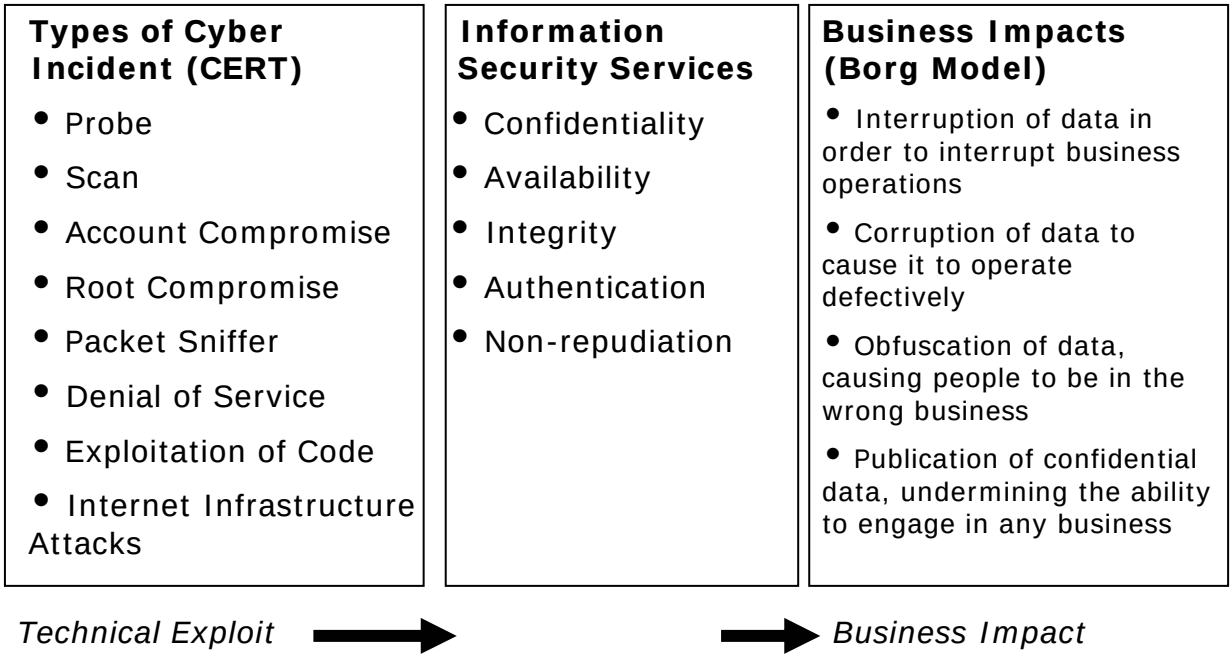
[4] "America At Risk: Closing the Security Gap", House Select Committee on Homeland Security, February 2004, pg. 87.

## CYBER VULNERABILTIES STUDY KEY FINDINGS

The Working Group supporting the Council's Prioritization of Cyber Vulnerabilities study set out to rank the impact cyber attacks would have on the various critical infrastructure sectors. The Working Group sought to gain information by conducting a survey of critical infrastructure companies.

### Methodology

The survey conducted by the group was based on a model espoused by Scott Borg, a former Senior Research Fellow at the Institute for Security Technology Studies, Dartmouth College. Using Borg's precepts, the group changed their focus from analyzing the impact that different "types" of cyber attacks could have on the various sectors, to trying to determine the economic consequences on a single firm that might result from a firm-specific hypothetical cyber attack.




- Column one provides examples of the **types of incidents** that could occur. Such incidents are routinely tracked by organizations, such as Computer Incident Response Team (CERT).[5]
- Column two summarizes the **security services** that a typical CIO works to ensure, these include confidentiality, availability, and integrity.
- Column three presents the possible **business impacts** (or consequences) of a given event.

For example, a **denial of service** attack could affect the availability of a network, resulting in an interruption of business operations. An **account compromise** could result in the insertion of

[5] A definition of the types of cyber attacks is included in Appendix A.

false data into a database, corrupting the integrity of the system's data. The resulting business impact could be the defective operation of the business. Through an **exploitation of code**, such as a virus, the availability of service may come into question. Such unreliability may deter people from using the service, which in the long-term, could drive companies out of business. An additional consequence of a cyber attack could be to undermine a system in a way that no one would use it. For example, if compromised, confidential information was publicized over the Internet, people would hesitate to use that source, due to the leak.

**Survey Respondents**

The Working Group selected survey participants that were considered large organizations, to provide a typical representative response from each sector. Surveys were sent to the CEOs of these major companies and the heads of government entities. Respondents described the impact of outages on three of their most critical network-based systems. Responding companies represented over $424 billion in 2003 revenue. Validation of the survey results was limited. Validation consisted of reviewing the responses of similarly situated companies to determine whether they had consistent approaches to answering the survey. The intent of the study was to obtain a high-level perspective of possible trends, so this approach was deemed appropriate.

The survey was sent to each critical infrastructure sector (including government). Responding sectors are listed in the below chart. No responses were received from the Agriculture and Food, Defense Industry, Chemical, and Government Emergency Services sectors, although surveys were sent to these sectors as well. The second column shows the number of responses received by sector, and the number of applications that were reviewed as part of the survey process. As stated above, these respondents represent over $424 billion in revenue for 2003:

| Sector | Respondents | Critical Systems Identified |
|---|---|---|
| Telecommunications | 2 | 6 |
| Information Technology | 2 | 6 |
| Transportation | 1 | 3 |
| Postal and Parcel Shipping | 1 | 3 |
| Banking and Finance | 6 | 18 |
| Public Health and Healthcare | 3 | 9 |
| Water | 1 | 3 |
| Energy | 3 | 9 |

For each type of attack, no specific mechanism used during the attack was defined, nor were sector-specific attacks defined. Respondents made whatever interpretations or assumptions they needed, in order to complete the survey.

The approach utilized to conduct the survey was to contact representatives at selected major companies or governmental entities who were considered to be representative of the sector, based on the knowledge of individuals in the Working Group. The selection was based on general knowledge that these large entities were typical of the sector; and it was therefore assumed that their responses would be representative of the sector. To validate this approach,

a review of the responses of "similarly-situated" companies was conducted to determine that they had consistent approaches to answering the survey. No further action was taken to validate the approach, given the time available. A more comprehensive survey that would engage all members of the sector might be undertaken if the Federal Government deems it appropriate and beneficial following this study.

**Survey Results**

**Note**: The NIAC Survey should be viewed as illustrative, rather than definitive due to the diversity of applications chosen per sector and the limited sample size. Also, it must be acknowledged that the answers provided are dependent upon the perspective of the respondent.

**Key Finding 1:**
**Dependency on network-based systems is pervasive across all sectors. Critical components of our national infrastructure rely on a variety of network-based systems.**

Results showed that dependency on network-based systems is pervasive across all sectors. Critical components of our national infrastructure rely on a variety of network-based systems. Examples of the various types of network-based systems that companies are using for critical business activities include control systems and customer service systems.

According to data collected by the Council, it became clear that a network installed by a major company in a sector is likely to rely on other computer systems to function. This trend of overlapping networks reveals the stark possibility that denying one aspect of a system could send ripple effects throughout the entire sector.

**Key Finding 2:**
**Each critical sector surveyed identified dependency on one or two sectors.**

One way to think about an answer to the President's question would be to recognize that a sector is as secure or as insecure as the common, shared infrastructure that sectors must use to operate network-based systems.

**Key Finding 3:**
**The answer to the question "are we ranking our critical infrastructures as to their vulnerability to cyber attacks" is multi-faceted. The degree that any sector is vulnerable is dependent upon a number of characteristics.**

These characteristics include:

- Type of Attack
- Scope of Impact
- Time of Attack
- Duration of Outage

Due to varying characteristics, it is difficult to provide a simple, concise answer to this question. The NIAC developed a methodology called the Common Vulnerability Scoring System (CVSS),[6] which could be used to prioritize responses to cyber incidents.

**Key Finding 4:**
**Sound business continuity practices, as well as information technology and cyber security best practices, provide some protection.**

The ability to revert to back-up systems or even manual systems, although less efficient, can minimize impact in some sectors. In many cases, redundancy expenses were already realized as part of existing business continuity programs. The results indicated the use of multiple vendors within core systems also provides additional protection.

[6] Common Vulnerability Scoring System (CVSS), National Infrastructure Advisory Council, October 12, 2004, http://www.dhs.gov/interweb/assetlibrary/NIAC_CVSS_FinalRpt_12-2-04.pdf

**RECOMMENDATIONS:**

**1. Direct lead agencies to work with each of the critical sectors to more closely examine the risks and vulnerabilities of providing critical services over network-based systems.**

In reviewing the findings with DHS and the Working Group, the Council recommends that continued work to investigate these types of issues would be beneficial. The Council would recommend that this type of work be done first at the sector level. The Sector Specific Agencies should help facilitate these efforts. While there are benefits to working across the sectors, there are also substantial benefits to further identify critical failure points within each sector. During a time of crisis, these critical areas could provide an indication of priority consideration, where appropriate.

**2. Direct DHS and the Sector Specific Agencies to identify potential failure points across Federal Government systems. Encourage the private sector to perform similar cross-sector analysis in collaboration with DHS, as long as DHS can assure protection of sensitive, proprietary results.**

The second recommendation flows from the first. There are critical applications within some companies in some sectors that can be thought of as potential points of failure. Companies should assess this risk and minimize it. The sectors and DHS should understand what failure points exist and work to mitigate issues around them. For example, mitigation strategies could include ensuring redundancy, either in the company or organization at issue or across the sector.

**3. Encourage sector and cross-sector coordinating groups (councils) to establish and/or support existing cyber security best practices or standards for their respective sectors.**

A number of sectors have established or adhere to corporate best practices with regard to cyber security issues and patch management. For example, the Energy Sector is working on "Cyber Security Standard 1300" within the electric utility area. The Financial Services Sector, through the BITS industry group, has developed a guide to telecommunication diversity and resiliency. Within the Telecommunications Sector, the Network Reliability and Interoperability Council (NRIC) have developed a series of Cyber Security Best Practices. The effectiveness of deploying these best practices should not be dismissed. For instance, companies that followed the NRIC's cyber security best practices avoided any significant impact from the Slammer virus.

**4. Direct DHS to sponsor cross-sector activities to promote a better understanding of the cross sector vulnerability impacts of a cyber attack.**

The thrust of this recommendation is to help each of the sectors better understand the impact of a cyber attack on their own sector, as well as the other sectors on which they depend. The best way to prepare for responding to a major cyber attack is to practice what they might do in such an event. DHS should provide a mechanism for a cross-section of key players in critical

sectors, as well as government and emergency services, to work through their roles in a recovery situation.

**5. Direct Federal agencies to include cyber attack scenarios and protective measures in their disaster recovery planning. Encourage sector coordinating groups to include cyber attack scenarios and protective measures in their disaster recovery planning**.

Federal agencies need to address cyber attacks in their own disaster recovery planning. In reviewing information on the SANS[7] Institute website, it was clear that government agencies are frequently targeted by hackers. For example, SANS Institute reported that 37 government or military sites were defaced within the 100 day period from August 2000 to November 2000. By spring 2001, one site a day was reported defaced.

Secondly, the Council recommends that the sector coordinating groups (councils) encourage the private companies they represent to include cyber attacks as a scenario they mitigate in their business recovery plans. The most effective way to learn how to deal with such an attack is through planning and practice.

**6. Encourage law enforcement organizations to prosecute cyber criminals and identity thieves, as well as publicize efforts to do so.**

The Council is encouraged that industry and the government are starting to see some positive developments in this area. For example, Microsoft established a $5 million fund to provide rewards for apprehending cyber criminals. This action led to the arrest of the creator of the Sasser Worm and NetSky virus, where a $250,000 reward was paid.

Unfortunately, there is also a trend in which the motive for hacking is moving away from a "leisure activity" to an opportunity to earn money illegally. Cyber crime has become a major tool of organized crime groups. A company recently reported that it is starting to see the use of bots to scan networks globally. For example, six arrests were made in four different countries where cyber criminals were used extortion to obtain $30,000 a month. A bot network consisting of more than 60,000 machines was used to track illegal gambling activities. The hackers then used information obtained from the bot network to blackmail gamblers.

In addition to the expense and productivity loss hackers create, it is also important from a strategic standpoint to be able to separate digital graffiti and crime from attacks that are sponsored by other governments and/or terrorists networks.

7. **Promote awareness of cyber security best practices at the corporate, government, small business, university, and individual levels.**

The Council's final recommendation is to promote awareness of cyber security best practices, at all levels. An example provided by SANS Institute showed the effectiveness that NASA had when it implemented an initiative to identify high priority vulnerabilities and address them.

[7] The SysAdmin, Audit, Network, Security (SANS) Institute

Through best practices, NASA was able to reduce the number of vulnerabilities on their 80,000 systems from 1.3 per machine, to less than .16 per machine, in 12 months. They continued to work this issue, and within the next 12 months, reduced it further to fewer than seven vulnerabilities per 1,000 systems.

Another example is the NRIC best practices for Cyber Security. Recall that the Slammer virus exploit occurred in January 2003; however, the patch to protect against that vulnerability was available 6 months earlier in July 2002. The Slammer virus did not impact companies that kept up-to-date with patch upgrades to applications. Security awareness and best practices must be practiced at all levels to effectively enhance the security of the overall Internet.

## Appendix A: Summary of Types of Cyber Attacks

**Probe -** A probe is characterized by unusual attempts to gain access to a system or to discover information about a system. One example is an attempt to log in to an unused account. Probing is the electronic equivalent of testing doorknobs to find an unlocked door for easy entry. Probes are sometimes followed by a more serious security event, but are often the result of curiosity or confusion.

**Scan -** A scan is a large number of probes done using an automated tool. Scans can sometimes be the result of an incorrect configuration or other error, but are often a prelude to a more directed attack on systems that the intruder found to be vulnerable.

**Account Compromise -** An account compromise is the unauthorized use of a computer account by someone other than the account owner, without involving system-level or root-level privileges (privileges a system administrator or network manager has). An account compromise might expose the victim to serious data loss, data theft, or theft of services. The lack of root-level access means, the damage can usually be contained, but a user-level account is often an entry point for greater access to the system.

**Root Compromise -** A root compromise is similar to an account compromise, except that the account that had been compromised has special privileges on the system. The term "root" is derived from an account on UNIX systems that typically has unlimited, or "superuser" privileges. Intruders who succeed in a root compromise can do just about anything on the victim's system, including run their own programs, change how the system works, and hide traces of their intrusion.

**Packet Sniffer -** A packet sniffer is a program that captures data from information packets as they travel over the network. This data may include usernames, passwords, and proprietary information that travels over the network in clear text. With perhaps hundreds of thousands of passwords captured by the sniffer, intruders can launch widespread attacks on systems. Installing a packet sniffer does not necessarily require privileged access. For most multi-user systems, the presence of a packet sniffer implies there has been a root compromise.

**Denial of Service -** The goal of denial of service attack is to prevent legitimate users of a service from using it, not to gain unauthorized access to machines or data. A denial of service attack can come in many forms. Attackers may "flood" a network with large volumes of data or deliberately consume scarce or limited resources, such as process control blocks or pending network connections. They may also disrupt physical components of the network or manipulate data in transit, including encrypted data.

**Exploitation of Trust -** Computers on networks often have trust relationships with one another. For example, before executing some commands, the computer checks a set of files that specify which other computers on the network are permitted to use those commands. If attackers can forge their identity, appearing to be using the trusted computer, they may gain unauthorized access to other computers.

**Malicious Code -** Malicious code is a general term for programs that, when executed, would cause undesired results on a system. Users of the system usually are not aware of the program until they discover the damage. Malicious code includes Trojan horses, viruses, and worms. Trojan horses and viruses are virtually hidden in legitimate programs or files attackers have altered to do more than what is expected. Worms are self-replicating programs that spread with no human intervention once they are started. Viruses are also self-replicating programs, but usually require some action on the part of the user to spread them inadvertently to other programs or systems. These sorts of programs can lead to serious data loss, downtime, denial of service, and other types of security incidents.

**Internet Infrastructure Attacks -** These attacks are rare and unlikely, but serious attacks involve key components of the Internet infrastructure rather than specific systems on the Internet. Examples are network name servers, network access providers, and large archive sites on which many users depend. Widespread automated attacks can also threaten the infrastructure. Infrastructure attacks affect a large portion of the Internet and seriously hinder the day- to-day operations of many sites.